



Ribbon Application Management Platform

Product Documentation Suite

Software Release: 24.12
Document Revision: 12.01
Published: 15 December 2024

Copyright

© 2020-2024 Ribbon Communications Operating Company, Inc. © 2020-2024 ECI Telecom Ltd. All rights reserved. The compilation (meaning the collection, arrangement and assembly) of all content on this site is protected by U.S. and international copyright laws and treaty provisions and may not be used, copied, reproduced, modified, published, uploaded, posted, transmitted or distributed in any way, without prior written consent of Ribbon Communications Inc.

Disclaimer and Restrictions

The publication is for information purposes only and is subject to change without notice. This publication does not constitute a commitment on the part of Ribbon. While reasonable efforts have been made in the preparation of this publication to assure its accuracy, Ribbon assumes no liability resulting from technical or editorial errors or omissions, or for any damages whatsoever resulting from the furnishing, performance, or use of the information contained herein. Ribbon reserves the right to make changes to this publication and to Ribbon products without notice in its sole discretion. This publication is not meant to define any interfaces between Ribbon products and any third-party hardware or software products.

Warranties

THIS INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL RIBBON BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR PERFORMANCE OF THIS INFORMATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Compliance with Applicable Laws and Export Control Laws

The information in this publication is subject to all applicable U.S. federal, state, and local laws. The customer use, distribution, and transfer of any technical information shall be in compliance with all applicable export and import laws and regulations. All Ribbon products and publications are commercial in nature; and the use, duplication, or disclosure by the United States Government is subject to the restrictions set forth in DFARS 252.227-7013 and FAR 52.227-19.

Trademarks

The trademarks, logos, service marks, trade names, and trade dress ("look and feel") on this website, including without limitation the RIBBON and RIBBON logo marks, are protected by applicable US and foreign trademark rights and other proprietary rights and are the property of Ribbon Communications Operating Company, Inc. or its affiliates. Any third-party trademarks, logos, service marks, trade names and trade dress may be the property of their respective owners. Any uses of the trademarks, logos, service marks, trade names, and trade dress without the prior written consent of Ribbon Communications Operating Company, Inc., its affiliates, or the third parties that own the proprietary rights, are expressly prohibited.

UNCONTROLLED COPY:

The original content is stored in an electronic database and is "write protected"; it may be altered only by authorized persons. While copies may be printed, it is not recommended. Viewing of the original content electronically ensures access to the current content. Any hardcopies taken must be regarded as uncontrolled copies.

Contents

Ribbon Application Management Platform 24.12	1
Getting Started	3
About RAMP	3
System Requirements	3
Resource Requirements.....	4
Environment-Specific Minimum Resource Requirements	5
Client Requirements	6
RAMP VNF deployment on KVM and VMware Platforms	6
Verifying the Disk Performance	8
Deployment Models.....	11
Standalone	11
Geographical Redundancy.....	12
Environments	13
Managed Devices.....	13
Features at a Glance	15
RAMP CNF - Introduction and Getting Started	17
RAMP CNF - Architecture	18
RAMP CNF - System Requirements	22
RAMP CNF - Changes to Existing RAMP Functionalities	28
RAMP CNF - Abbreviations and Terminologies.....	30
RAMP CNF - Resiliency	35
RAMP CNF - Observability.....	118
RAMP CNF - Performance Metrics	123
Installation and Upgrade Guide	125
Installing RAMP	125
Hostname and Instance Name Conventions.....	126
Installing RAMP in Virtual and Private Cloud Environments	127
Installing RAMP in Public Cloud Environments.....	202
Installing RAMP CNF	251
Install and Configure Ribbon OEM Host OS for RAMP on Dell Server.....	284
RAMP Customization for Docker Daemon	285
Upgrading RAMP	301
Pre-Upgrade Checklist	302
Upgrading RAMP in Virtual and Private Cloud Environments.....	304

Upgrading RAMP in Public Cloud Environments	325
Upgrading RAMP CNF	330
Post-Upgrade Procedures for RAMP	374
Migrating to RAMP	376
Migrate EdgeView to RAMP	376
Migrate Insight EMS to RAMP	377
Installing etcd	387
Installing etcd on Kubernetes	388
Installing etcd on KVM.....	426
Installing etcd on OpenStack.....	441
Installing etcd on VMware	456
Upgrading etcd	459
Upgrading etcd on KVM	460
Upgrading etcd on VMware	476
Upgrading etcd on Openstack.....	477
Upgrading etcd on Kubernetes.....	478
Health Check etcd	508
Rolling Back RAMP CNF.....	508
Uninstalling RAMP CNF	509
RAMP CNF - Uninstall Using Git.....	509
RAMP CNF - Uninstall Using Helm Commands.....	510
RAMP CNF - Delete PVCs.....	511
RAMP User Guide.....	513
How to Access RAMP	513
GUI	513
REST API	513
Command Line Interface	513
Device CLI Through RAMP	514
System Requirements to Access RAMP on a Web Browser.....	514
Log onto the RAMP GUI.....	515
Log onto the RAMP CLI	516
Getting Started with the RAMP User Interface.....	518
Dashboard	518
Navigation Menu	522
Global Search Service.....	526
System Menu	528

Table Controls	530
Customize the Logon Banner	533
Device Management	533
Device Registration on RAMP	534
Registering Devices on RAMP	535
Manage Registered Nodes.....	663
Manage Clusters	694
Launching Device GUIs from RAMP	699
Work with Resource Groups	808
Work with Inventory Reports	811
Modify Managed Device Association.....	815
Configure Device Management Administration Options.....	816
Firmware Repositories	818
Device Operations.....	820
GSX CLI Through RAMP	821
Enabling Deprecated Algorithms for RAMP CLI	823
RESTCONF API for SBC Core.....	824
SOAP API for SBC Core	827
SOAP API for PSX.....	854
PSX CLI Through RAMP	855
SBC CLI Through RAMP	857
Provision SBC Devices	860
Back Up and Restore SBC and SLB Devices	866
Upgrade SBC Devices	871
Generate Health Reports	875
Lock and Unlock Devices	877
Automate Configuration Tasks for GSX.....	878
GSX Upgrade Automation	953
Authentication and Authorization.....	964
Authentication Methods RAMP Supports.....	964
RAMP's Authorization Model	966
Multi-Tenancy Support (Optional).....	967
Authentication and Authorization Workflows	968
Configure Multi-Tenancy.....	969
Add Users.....	969
Add User Groups.....	976

Configure Authentication Methods	977
Locations	998
Manage Certificates	999
Monitor User Activity	1000
Terminate User Sessions	1001
Set Session Expiry in RAMP GUI	1001
Authentication and Authorization Administration	1001
EdgeView Service Administration	1003
License Management	1004
Licensing Models	1004
Planning for License Management	1007
Installing Licenses	1007
Associating Licenses with Devices	1007
Monitoring License Status and Usage	1008
Usage Reports for Post-Paid Billing	1009
License Management Workflows	1009
Find License Keys for Obtaining Licenses	1010
Obtain Licenses	1011
Install Licenses	1012
Activate Licenses	1012
Revoke Licenses	1018
Set Alerts for License Expiry	1019
Set Up Reporting for Post-Paid Billing	1019
Monitor License Usage	1024
Licensed Feature on RAMP	1029
Performance Management	1054
Planning for Performance Management	1054
Define Which Statistics to Collect	1055
Define Which Statistics to Export	1055
Specify How Long to Retain Statistics Data	1055
Enable Statistics Collection and Exporting	1055
Generate PM Reports and Report Templates	1056
Define Statistics Values that Trigger Alarms	1056
Performance Management Workflows	1056
Collect and Export Device Statistics	1057
Working with Reports	1078

Define Performance Thresholds.....	1082
Exported Statistics.....	1084
RAMP System Configuration.....	2077
System Registration	2077
Application Configuration	2078
Change IP Address	2101
System Activity Logging	2102
Exporting Logs to a Remote Syslog Server	2103
Device REST Credentials.....	2108
SSH Active Channels	2109
RAMP Profile Settings	2109
Database Configuration.....	2110
PSX Call Trace Destination	2110
PSX Manager Version Compatibility	2111
GSX User Interface	2111
SSH Configuration.....	2114
RAMP Tools.....	2115
Call Trace	2116
Call History	2117
Inventory.....	2121
Report Scheduler	2123
Trunk Group	2134
GSX System.....	2155
Number Portability Services	2156
Joint Interoperability Test Command	2170
Workflow to Deploy JITC on RAMP	2171
Update the Configuration File for JITC	2174
Configure RAMP GUI to Comply with JITC	2180
Configure RAMP for TLS Communication.....	2185
Configure NTP Server Authentication	2187
Notifications.....	2187
Security Best Practices	2190
RAMP Security Best Practices Introduction	2190
Security Concerns	2190
Managing RAMP Users and Accounts	2191
Use a Master-Key to Encrypt RAMP Passwords	2192

Follow Standard Linux Password Guidelines	2192
Change Any Default Passwords	2192
Manage Administrative Accounts	2192
Avoid Customization of the Linux Environment	2192
Managing RAMP Network Security	2193
RAMP Secure Network Configuration	2193
Certificate Management	2210
RAMP Event Logging for Security	2210
System Activity Logs	2211
User Activity Logs	2211
Web Request Logs	2211
API and CLI Usage Logs	2211
Remote Syslog	2211
SFTP File Transfer Logs	2212
Configuring RAMP Redundancy	2213
Generate Redundancy Templates	2213
Configuring RAMP GR	2217
Configuring RAMP GR with Automatic Switchover Enabled	2220
Generate a Redundancy Template	2222
Configure RAMP GR Parameters	2224
Setting Up an etcd Cluster	2226
Lawful Intercept Guide	2284
Ribbon Lawful Intercept Overview	2284
Ribbon Lawful Intercept Topology	2285
Lawful Intercept for RAMP	2287
Lawful Interface Architecture	2288
Enabling Lawful Intercept on RAMP	2288
Configuring Call Data Channel	2289
Configure CDC for All Nodes	2291
Configure CDC for GSX Nodes	2293
Configure CDC for SBC Core Nodes	2294
Managing Mediation Servers	2322
Create a Mediation Server	2323
Importing TLS Security Certificate to RAMP	2325
Provisioning LI Targets	2326
Overview	2327

Provisioning Limitations.....	2328
Target Provisioning Sequence.....	2328
Apply Restrictions on Lawful Intercept Targets	2343
Call Processing	2344
Call Data Interface.....	2344
Call Content Interface.....	2349
GSX Lawful Intercept Basic Call Processing.....	2349
SBC Lawful Intercept Basic Call Processing.....	2351
Viewing CDC Status Report	2352
View GSX CDC Report Using CLI.....	2353
LI Performance Management.....	2353
GSX LI Performance Reports.....	2354
SBC LI Performance Reports.....	2361
LI Fault Management	2361
GSX Lawful Intercept Alarms	2361
SBC Lawful Intercept Alarms.....	2363
RAMP Lawful Intercept Alarms.....	2363
LI Security	2365
Separate LI Provisioning and System Management	2365
Provisioning Only via API from Intercept Server	2365
Write-Only RAMP LI Provisioning.....	2366
PSX Security	2366
IS Handling of Ribbon IP Addresses	2366
GSX and SBC Handling of Call Content IP Address	2366
Billing	2366
Protocol Security	2366
Deploying liTestWebApp in RAMP	2366
Related Documentation.....	2367
Alarms and Troubleshooting.....	2368
RAMP Alarms Guide	2368
New and Deprecated Alarms.....	2369
Managing Device Faults.....	2370
RAMP Alarms	2371
Cross-Platform Alarms	2486
Fault Management	2522
Planning for Fault Management	2523

Enable Sending Alarms from Devices to RAMP	2523
Customize the Alarm Interface	2523
Work with Active Alarms on the FM Dashboard	2523
View Alarm History	2524
Reclassify the Alarm Content	2524
Send Email Notifications	2524
Send Alarms to an External Destination	2524
Administer Fault Management	2524
Fault Management Workflows	2525
Work with Active Alarms	2526
Work with Alarm History	2535
Purge Alarms	2535
Reclassify Alarm Content	2537
Send Email Notifications for Alarms	2537
Forward Alarms to an External Destination	2541
Monitor Fault Management Activity	2550
Troubleshooting Guide	2551
EdgeMarc Troubleshooting	2551
Database Troubleshooting	2566
Fault Manager Troubleshooting	2568
General Troubleshooting	2569
GSX Troubleshooting	2572
RAMP CNF Troubleshooting	2578
RAMP GR Auto-Switchover Troubleshooting	2584
Retrieve System Information	2593
Tools Troubleshooting	2597
Unlock or Recover a User Account for Sysadmin or Any Admin User	2598
Administration Guide	2601
Accessing RAMP VNF Using Active Directory	2602
Configure the Linux System	2603
Reconfiguring Active Directory	2619
Accessing RAMP CNF Using Active Directory	2621
Configure the Linux System	2622
Custom Host and DNS Configuration for Kubernetes Pods	2634
Daily Maintenance Activities	2635
Continuous Monitoring	2636

Daily Maintenance Tasks.....	2636
Daily Database Backups	2636
How to Start and Stop RAMP	2636
Start RAMP	2636
Stop RAMP	2636
How to Start and Stop Sonus Agent.....	2636
How to Rediscover the localhost.....	2637
How to Control the Network Range.....	2638
How to Prepare RAMP for ROHOS Upgrade.....	2639
Access RAMP Database	2640
Attach RAMP to Multiple Disjointed IP Networks	2641
Using RAMP as a PSX Proxy.....	2642
Separation of OAM and Signaling Networks on Call Trace in RAMP	2647
Backup and Restore.....	2648
Take a Backup of RAMP for Daily Maintenance.....	2648
Take a Backup of RAMP for Upgrade	2654
Restore from Backup on RAMP Standalone	2659
Restore from Backup on RAMP GR.....	2661
Restore a Master Key File.....	2663
Restore a Master Key File (.KF) Manually	2664
Check Software Versions	2666
Check RAMP Version	2666
Check LINTel Platform Version in RAMP	2666
Check Red Hat Enterprise Linux Server Version in RAMP	2667
Check PostgreSQL Version in RAMP	2667
Check Java Version in RAMP	2667
Check DBaaS Version in RAMP.....	2668
Check Platform Kernel Version in RAMP	2668
Check Status	2668
Check RAMP Status.....	2669
Check Deployment Status of Services in RAMP.....	2670
Change Time Zone on RAMP	2670
Deploy Optional Services on RAMP.....	2671
Deploy the Action Service	2671
Backup/ Restore/ Upgrade	2672
Deploy the EdgeView Service	2672

Deploy the Object Store Service	2673
Download Files from Ribbon Support Portal	2673
Export the RAMP Configuration Tables	2676
Schedule a Cron Job Automatically.....	2678
Export the Configuration Table Automatically.....	2679
Install PSX Manager on RAMP	2683
Managing Accounts and Passwords	2685
Manage RAMP Account Names and Passwords	2686
Manage User Accounts	2709
Establish Passwordless Connection from an External Server to RAMP	2713
Establish RAMP CNF Active-Standby Instance Passwordless Connection	2714
Change the GRUB Password.....	2715
Managing Log Files	2716
Change Log Level	2716
Configure Silent Auth for Jboss CLI	2738
RAMP Log Files.....	2740
Reset Admin Password for Jboss CLI	2774
Managing the NTP Server	2775
Add Multiple NTP Servers for RAMP	2775
Synchronize RAMP with the NTP Server	2776
Managing Redundancy	2777
Check Database and File Replication Status.....	2778
Change the Role of a Node in RAMP GR	2778
Reconfigure a Standby Node in RAMP GR.....	2779
Tear Down RAMP GR	2780
Replace a Node in RAMP GR	2782
Managing Resources	2783
Manage Resources for RAMP on KVM.....	2784
Manage Resources for RAMP on OpenStack.....	2787
Manage Resources for RAMP on VMware ESXi	2789
Managing Secure Communications	2790
Secure Login to the RAMP GUI	2790
Secure Communication Between RAMP and Devices.....	2803
Enable Key-Based Authentication for SSH	2815
Manually Generate Traps and Verify Alarm Handling	2819
Parse MIB to JSON/HTML	2820

Generate Traps	2824
Configure SNMPv3 Receiver Using snmptrapd to Test SNMPv3 Traps	2826
Proxy Manager	2827
Legacy Device Management.....	2828
Revert Procedure	2830
REST API Documentation.....	2832
Accessing the API Documentation from RAMP.....	2832
View RAMP API User Documentation	2833
Download RAMP API Definition Files	2833
Authentication Requirements	2833
Obtain a Token Using a Username and Password.....	2833
Obtain a Token using a SAML Service Provider.....	2834
Refresh an Authentication Token.....	2834
Role-Based User Access Requirements	2835
Terminating a Session	2835
Example API Requests and Responses.....	2835
User Authentication Using a Password	2836
Retrieve the List of User Roles.....	2838
Add a Collection Profile	2839
Change Collection Profile Assignment	2842
Retrieve Usage Level for a Licensed Feature	2844
Configure OSS Trap Resync Parameters	2845
RAMP Release Information	2847
Ribbon Application Management Platform 24.12R0 Release Notes	2847
About Ribbon Application Management Platform Release Notes	2847
Ribbon Application Management Platform	2848
New Features and Functionalities	2850
SOAP API Deprecation Notice	2851
Security Vulnerabilities	2851
Hardware and Software Requirements	2852
Upgrade Notes	2855
Migration Notes	2855
Checksums and ID Details	2856
Resolved Issues	2857
Known Issues	2881
Known Limitations	2889

New in RAMP 24.12.00R000	2889

Ribbon Application Management Platform 24.12

Ribbon Application Management Platform (RAMP)



Getting Started

- [About RAMP](#)
- [System Requirements](#)
- [Verifying the Disk Performance](#)
- [Deployment Models](#)
- [Managed Devices](#)
- [Features at a Glance](#)
- [RAMP CNF - Introduction and Getting Started](#)

Installation and Upgrade Guide

- [Installing RAMP](#)
- [Upgrading RAMP](#)
- [Migrating to RAMP](#)
- [Installing etcd](#)
- [Upgrading etcd](#)
- [Health Check etcd](#)
- [Rolling Back RAMP CNF](#)
- [Uninstalling RAMP CNF](#)

User Guide

- [How to Access RAMP](#)
- [Getting Started with the RAMP User Interface](#)
- [Device Management](#)
- [Device Operations](#)
- [Authentication and Authorization](#)
- [License Management](#)
- [Performance Management](#)
- [RAMP System Configuration](#)
- [RAMP Tools](#)
- [Joint Interoperability Test Command](#)
- [Notifications](#)

Administration Guide

- [Accessing RAMP VNF Using Active Directory](#)
- [Accessing RAMP CNF Using Active Directory](#)
- [Daily Maintenance Activities](#)
- [How to Start and Stop RAMP](#)
- [How to Start and Stop Sonus Agent](#)
- [How to Rediscover the localhost](#)
- [How to Control the Network Range](#)
- [How to Prepare RAMP for ROHOS Upgrade](#)
- [Access RAMP Database](#)
- [Attach RAMP to Multiple Disjointed IP Networks](#)
- [Backup and Restore](#)
- [Check Software Versions](#)
- [Check Status](#)
- [Change Time Zone on RAMP](#)
- [Deploy Optional Services on RAMP](#)
- [Download Files from Ribbon Support Portal](#)
- [Export the RAMP Configuration Tables](#)
- [Install PSX Manager on RAMP](#)

Security Best Practices

- [RAMP Security Best Practices Introduction](#)
- [Managing RAMP Users and Accounts](#)
- [Managing RAMP Network Security](#)

- [Certificate Management](#)
- [RAMP Event Logging for Security](#)

Alarms and Troubleshooting

- [RAMP Alarms Guide](#)
 - [New and Deprecated Alarms](#)
 - [Managing Device Faults](#)
 - [RAMP Alarms](#)
 - [Cross-Platform Alarms](#)
- [Fault Management](#)
 - [Fault Management Workflows](#)
 - [Work with Active Alarms](#)
 - [Work with Alarm History](#)
 - [Purge Alarms](#)
 - [Reclassify Alarm Content](#)
 - [Send Email Notifications for Alarms](#)
 - [Forward Alarms to an External Destination](#)
 - [Monitor Fault Management Activity](#)
- [Troubleshooting Guide](#)
 - [EdgeMarc Troubleshooting](#)
 - [Database Troubleshooting](#)
 - [Fault Manager Troubleshooting](#)
 - [General Troubleshooting](#)
 - [GSX Troubleshooting](#)
 - [RAMP CNF Troubleshooting](#)
 - [RAMP GR Auto-Switchover Troubleshooting](#)
 - [Retrieve System Information](#)
 - [Tools Troubleshooting](#)
 - [Unlock or Recover a User Account for Sysadmin or Any Admin User](#)

- [Managing Accounts and Passwords](#)
- [Managing Log Files](#)
- [Managing the NTP Server](#)
- [Managing Redundancy](#)
- [Managing Resources](#)
- [Managing Secure Communications](#)
- [Manually Generate Traps and Verify Alarm Handling](#)
- [Proxy Manager](#)
- [Legacy Device Management](#)

Lawful Intercept Guide

- [Ribbon Lawful Intercept Overview](#)
- [Lawful Intercept for RAMP](#)
- [Enabling Lawful Intercept on RAMP](#)
- [Configuring Call Data Channel](#)
- [Managing Mediation Servers](#)
- [Provisioning LI Targets](#)
- [Call Processing](#)
- [Viewing CDC Status Report](#)
- [LI Performance Management](#)
- [LI Fault Management](#)
- [LI Security](#)
- [Deploying liTestWebApp in RAMP](#)
- [Related Documentation](#)

Additional Documentation

- [REST API Documentation](#)
- [Ribbon Product Interoperability](#)
- [Open Source Attribution Documents](#)
- [How to Search in Wiki](#)

RAMP Releases

- [Ribbon Application Management Platform 24.12R0 Release Notes](#)

Getting Started

Contents

- [About RAMP](#)
- [System Requirements](#)
- [Verifying the Disk Performance](#)
- [Deployment Models](#)
- [Managed Devices](#)
- [Features at a Glance](#)
- [RAMP CNF - Introduction and Getting Started](#)
 - [RAMP CNF - Architecture](#)
 - [RAMP CNF - System Requirements](#)
 - [RAMP CNF - Changes to Existing RAMP Functionalities](#)
 - [RAMP CNF - Abbreviations and Terminologies](#)
 - [RAMP CNF - Resiliency](#)
 - [RAMP CNF - Observability](#)
 - [RAMP CNF - Performance Metrics](#)

About RAMP

The Ribbon Application Management Platform (RAMP) is a centralized management client for Ribbon devices in a customer's network. These devices include:

- Session Border Controller (SBC) Core
- SBC Edge
- Policy Server (PSX)
- Gateway Server (GSX)
- Signaling Gateway (SGX)
- Diameter Signaling Controller (DSC)
- Data Stream Integrator (DSI)
- Media Resource Function Processor (MRFP)

The RAMP provides a complete Fault, Configuration, Accounting, Performance, and Security solution with a portfolio of management and provisioning tools. The RAMP provides a range of software and network management functions for virtualized and cloud-based Ribbon devices. It provides registration services that bring devices into the managed network and offers features to facilitate device configuration and software management.

Support personnel in a network operations center (NOC) log on to the RAMP to manage Ribbon devices. The RAMP users can be distributed across geographical locations. The RAMP provides a northbound REST API for provisioning integration and northbound and southbound SNMPv3 support for trap forwarding.

There is an option to integrate the RAMP with external applications such as an Operational Support System (OSS).

System Requirements

In this section:

- [Resource Requirements](#)
- [Environment-Specific Minimum Resource Requirements](#)
- [Client Requirements](#)
- [RAMP VNF deployment on KVM and VMware Platforms](#)

The system requirements for deploying Ribbon Application Management Platform (RAMP) are described here.

Resource Requirements

The minimum resource requirements for a single RAMP instance are covered in this table. For RAMP GR, use two instances with this configuration.

For supported deployment models on every environment, refer to [Deployment Models](#).

Resource	Environment					
	KVM	VMware ESXi	OpenStack	Azure	AWS	CNF
Disk (GB)	300		150 (HDD) + 450 (external volume)			130 (HDD) + 490 (external volume)
RAM (GB)	64					72
vCPU	16					20
vNIC	1 or 2*					

Note

These requirements refer to the RAMP deployment only. For KVM and VMware deployments, Ribbon recommends ensuring a minimum of 2 vCPUs plus 16 GB of RAM is available (Not shared with the guest instances) for the environment.

To enable automatic failover on RAMP, additional three etcd Virtual Machines are required. For etcd resource requirement, refer to [RAMP etcd System Requirements](#).

Note

Ensure the vCPUs are in a single NUMA (Non Uniform Memory Access). If 16 vCPUs are not available in a single NUMA, split it across multiple NUMAs.

For example, When the Host includes 60 vCPUs with 2 NUMAs, allocate all RAMP 16 vCPUs in the same NUMA (16 vCPUs and 16 cores per socket). If NUMAs are not available and when the Host includes 20 vCPUs with 2 NUMAs, allocate all 16 RAMP vCPUs from both NUMAs. (16 vCPUs and 8 cores per socket).

Reservation: Set the CPU reservation to half the number of vCPUs assigned to the VM multiplied by the physical CPU processor speed.

For example, for a configuration of 16 vCPUs with a processor speed of 2.992 GHz CPU frequency, reserve "2992 * 8 = 23936 MHz".

Environment-Specific Minimum Resource Requirements

Environment-specific minimum resource requirements for RAMP are covered in this table.

Environment	Resource	Version			
KVM	KVM (Kernel Virtual Machine)	3.10.0			
	Compilation library	libvirtd 4.5.0			
	Library	libvirtd 4.5.0			
	API	QEMU 4.5.0			
	Hypervisor	QEMU 1.5.3			
VMware	VMware ESXi	6.5	6.7	7.0	8.0
	Virtual Machine	13	14	14	14
	Hard Disk Type	Thick provisioned, lazily zeroed.			
OpenStack	Red Hat OpenStack Platform (RHOP)/ Host operating system	• 10 / RHEL 7.3 • 13 / RHEL 7.5 • 16, 16.1, 17, 17.1/ RHEL 8.1			

Environment	Resource	Version
AWS	- The system hosting AWS requires a disk with a minimum size of 150 GB. - Instance type (flavor): one which meets the requirements above. example: m5.4xlarge - The newer generation M5 instance underlying the Hypervisor is KVM Nitrox and Networking is ENA.	

Client Requirements

The following table lists the requirements to access RAMP through a web browser:

Operating system	Windows 10
Web browser	- Microsoft Edge 126.0 - Chrome version 126.0 - Mozilla Firefox 127.0 Note Enable TLS 1.2 or TLS 1.3 in the web browser to access RAMP.
Plug-in	Java 1.8 or higher version (required to support PSX Manager) Note If you do not have the latest Java version, warnings messages display when you attempt to access PSX Manager through RAMP.

RAMP VNF deployment on KVM and VMware Platforms

The following tables lists the disk type requirements for RAMP VNF deployments for KVM and VMware platforms:

Note

- **Server Storage:** For optimal performance, the RAMP recommends servers with SSD disks.
- **Disk Type:** SSD (Highly recommended) for KVM and VMware platforms.

Ensure the disk meets the IOPS criteria on the [Verifying the Disk Performance](#).

The following are the SSD requirements for Sequential Read:

Disk Type	Host Type	Sequential Read	
SSD	VMware	IOPS*	Bandwidth**
		111k	453 MB/s
		*The average I/Os performed per second **The average bandwidth rate shown as value in power of 10 format	
SSD	KVM	IOPS*	Bandwidth**
		474k	1943 MB/s
		*The average I/Os performed per second **The average bandwidth rate shown as value in power of 10 format	

SSD requirements for Random Read:

Disk Type	Host Type	Random Read	
SSD	VMware	IOPS*	Bandwidth**
		6108	25 MB/s
		*The average I/Os performed per second **The average bandwidth rate shown as value in power of 10 format	

Disk Type	Host Type	Random Read	
SSD	KVM	IOPS*	Bandwidth**
		11.2k	45 MB/s
		*The average I/Os performed per second **The average bandwidth rate shown as value in power of 10 format	

Verifying the Disk Performance

The RAMP VNF may experience issues if it encounters poor IOPS (Input/Output Operations per second) performance of its storage devices. The Ribbon Application Management Platform (RAMP) allows you to measure the storage performance (disk I/O speed) for the RAMP installed on KVM and VMware platforms.

Prerequisites

The host configuration runs the `Hostchecker` script file. For more information on the `Hostchecker` utility, refer to [Check KVM Host System Requirements](#).

Fio Utility

The `fio` (Flexible I/O Tester) utility uses the `fio` disk benchmarking tools to measure the persistent disk performance. The tools measure IOPS (Input Output Operations per Second) and throughput for realistic workloads.

Note

While managing a Linux server, particularly in contexts involving databases, virtualization, or any I/O-intensive tasks, it is essential to understand the performance of your storage device. A highly reliable tool for this purpose is `fio` (Flexible I/O Tester). It simulates a wide range of I/O workloads to evaluate the performance of your storage devices.

Note

The `write fio` (Flexible I/O Tester) offers write commands (random and sequential). However, over a period of time, the `fio` can corrupt the OS files. Thus, the `write fio` is not used in this document.

Perform the following procedure to verify if the disk performance meets the minimum expected performance based on the benchmarks performed by Ribbon.

Start

1. Log on to the RAMP CLI as `root` user. For more information, refer to [Log onto the RAMP CLI](#).
2. Check if the `fio` is installed on the system:

```
yum list installed | grep fio
```

3. To check the `fio` version:

```
fio --version
```

4. If `fio` is not installed, install using:

```
yum -y install fio
```

RAMP should have public access/repository configured to install fio package.

5. Read the throughput by performing the Sequential Read:

Note

<filename> for **KVM** must be " /dev/vda2 " and for **VMware** must be " /dev/sda2 "

```
fio --name=[global] --ioengine=libaio --filename=<filename> --iodepth=128 --rw=read --bs=4k --direct=1 --numjobs=16 --runtime=10 --group_reporting
```

The following table depicts the SSD disc performance benchmarking values for Sequential Read:

Disk Type	Host Type	Sequential Read	
SSD	VMware	IOPS*	Bandwidth**
		111k	453 MB/s
		*The average I/Os performed per second. **The average bandwidth rate shown as value in power of 10 format.	

Disk Type	Host Type	Sequential Read	
SSD	KVM	IOPS*	Bandwidth**
		474k	1943 MB/s
		*The average I/Os performed per second. **The average bandwidth rate shown as value in power of 10 format.	

6. Read the throughput by performing the Random Read:

Note

<filename> for:

- **KVM** must be /dev/vda2
- **VMware** must be /dev/sda2

```
fio --name=[global] --ioengine=libaio --filename=<filename> --iodepth=128 --
rw=randread --bs=4k --direct=1 --numjobs=16 --runtime=10 --group_reporting
```

The following table depicts the SSD disc performance benchmarking values for Random Read:

Disk Type	Host Type	Random Read	
SSD	VMware	IOPS*	Bandwidth**
		6108	25 MB/s
		*The average I/Os performed per second. **The average bandwidth rate shown as value in power of 10 format.	
SSD	KVM	IOPS*	Bandwidth**
		11.2k	45 MB/s
		*The average I/Os performed per second. **The average bandwidth rate shown as value in power of 10 format.	

Note

Even though the `fio` (Flexible I/O Tester) benchmarking may help uncover issues at install time (without an actual running load), it is only indicative. Running `fio` (Flexible I/O Tester) over a long period with a real load, and in a specific environment and deployment type (RAMP alone or RAMP with SBC and PSX, and so on), provides more valuable information about the level of system performance.

Deployment Models

In this section:

- [Standalone](#)
- [Geographical Redundancy](#)
- [Environments](#)
 - [On a Dedicated Server](#)
 - [Public Cloud](#)
 - [Private Cloud](#)

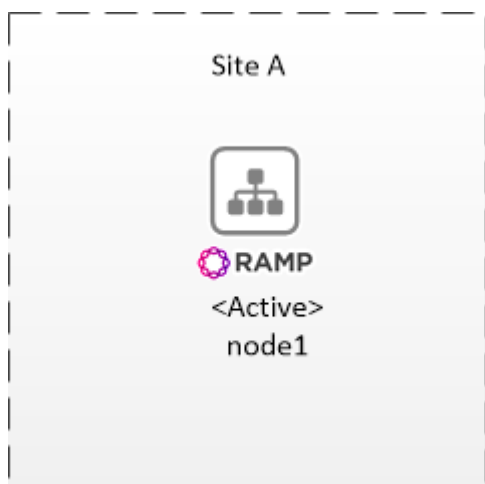
Ribbon Application Management Platform (RAMP) software runs as a virtual machine (VM) or virtual network function (VNF) in various virtualized/cloud environments. As a software-based application, RAMP decouples the features and functionality from proprietary hardware and greatly expands the options for where and how RAMP is deployed.

The software-based nature of RAMP enables great flexibility in network design. Operators select the environment and determine the number and size of RAMP instances, or nodes, they need to meet their requirements. Working with virtual instances, an operator can readily adapt the deployment capacities by creating or tearing down RAMP devices as their requirements change.

The RAMP deployment models are covered in this section.

Standalone

RAMP standalone (SA) consists of one RAMP node.



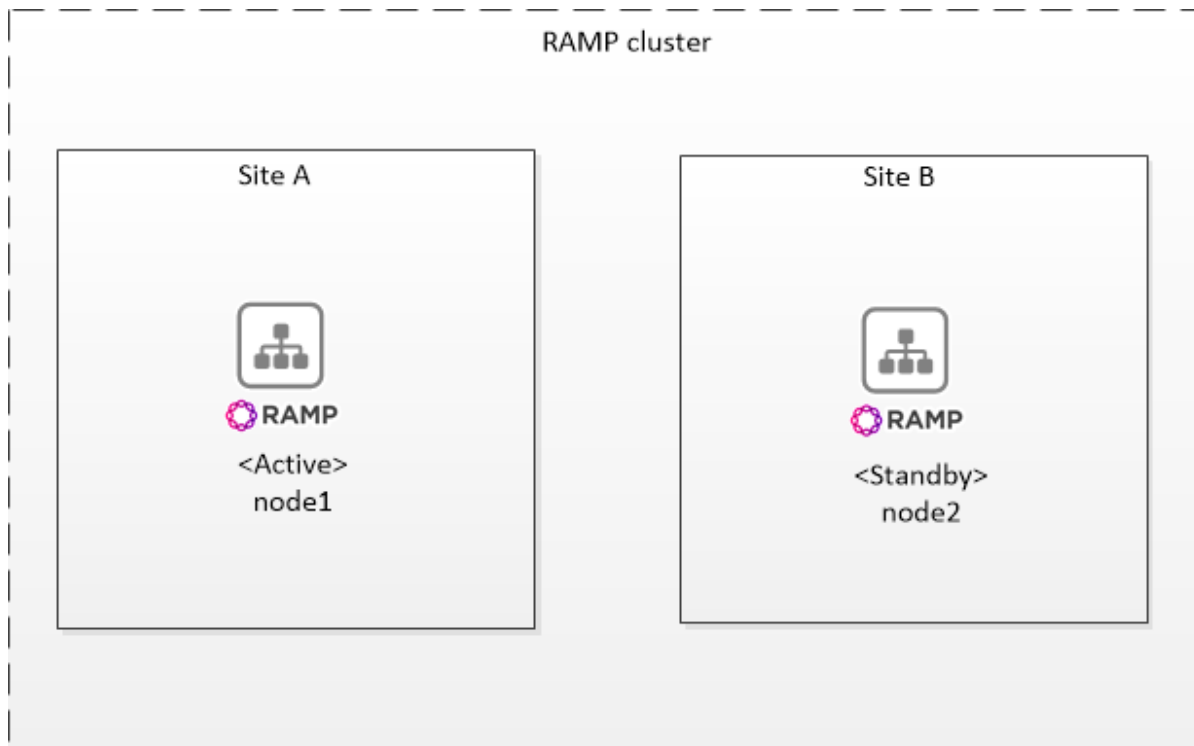
One instance of every microservice (MS) runs in the RAMP node.

Geographical Redundancy

RAMP Geographical Redundancy (GR) consists of two RAMP nodes in two sites at geographically different locations providing data and service replication.

Note

The recommended delay between two GR sites is 60 ms.



In a RAMP GR deployment, data is synced between Site-A and Site-B. Microservices run in both the active and standby RAMP nodes.

- Site-A is the primary site that performs all the active processing.
- Site-B is a cold standby site that receives replicated data from the primary active site.

GR supports both manual and automatic switchover. If the RAMP at Site-A goes down, you can manually activate the RAMP at Site-B. It is primarily useful when there is a catastrophic failure or, for some other reason, only one data center is impacted. The data is already available at the data center in Site-B and application services are restored upon doing a failover from the data center at Site-A. GR deployments provide other benefits such as initiating a planned switchover of services to the data center at Site-B, if there is a maintenance activity planned at the data center in Site-A.

As an alternative to initiating manual switchovers, RAMP also supports a deployment model that enables automatic switchover between GR instances. To enable automatic switchover, deploy three additional VMs, each running an instance of `etcd`. The `etcd` instances constantly monitor whether they are able to communicate with the RAMP instances and use that information to function as arbitrators that determine which RAMP instance should be active. A switchover occurs automatically when most of the `etcd` instances determine the current

active instance is no longer reachable. For more information, refer to [Configuring RAMP GR with Automatic Switchover Enabled](#).

Environments

This section covers the RAMP deployment models supported in each environment.

RAMP deployment models and environments

Deployment model	Environment					
	KVM	VMware ESXi	OpenStack	Azure	AWS	CNF
SA	✓	✓	✓	✓	✓	✓
GR	✓	✓	✓			✓

For more information on the RAMP CNF architecture, refer to [RAMP CNF - Architecture](#).

On a Dedicated Server

RAMP is deployed as a VM on commercial off-the-shelf (COTS) hardware equipped with a hypervisor, such as a VMWare ESXi or KVM environment.

The following environments are supported:

- x86_64 Linux with KVM Hypervisor
- x86_64 compatible server running VMware ESXi version 6.7.0 or later

Public Cloud

RAMP is deployed as a VNF in a public cloud environment such as Amazon Web Services (AWS) and Microsoft Azure.

Private Cloud

RAMP is deployable as a CNF in an enterprise Kubernetes cluster.

Managed Devices

The Ribbon Application Management Platform (RAMP) manages the following devices:

Device type	Variants	Interfaces supported			
		GUI	CLI	SOAP API	REST/RESTCONF API
Application Server	• AS	✓			

Device type	Variants	Interfaces supported			
		GUI	CLI	SOAP API	REST/RESTCONF API
Centralized Policy and Routing Server	• PSX SWe • PSX CNe	✓	✓	✓	
DataStream Integrator Call Data Record Translation Engine	• DSI • DSI SWe	✓			
Diameter Signaling Controller	• DSC 8000 • DSC SWe	✓			
Edge 8000	• 8100 • 8300	✓			
EdgeMarc	• 7000 • 4800 • 2900	✓			
GSX9000 High-density Media Gateway Open Services Switch (NFS)	• GSX9000	✓	✓		
Identity Hub	• IDH	✓			
MRFP	• MRFP	✓	✓		✓
NTR Devices	• C3 G9EMS • C20 • G5 • G6MM • GMS • L2MGR	✓			
SBC Core	• SBC 5400 • SBC 7000 • SBC SWe • SBC CNe	✓	✓		✓
SBC Edge	• SBC 1000 • SBC 2000 • SBC SWe Edge	✓			

Device type	Variants	Interfaces supported			
		GUI	CLI	SOA P API	REST/ RESTCO NF API
SGX4000 Universal Signaling Gateway	• SGX4000	✓			
SIP Load Balancer	• SLB	✓	✓		✓
STI	• STI	✓			

The RAMP supports manual, dynamic, and automatic registration of the managed devices. For more information, refer to [Device Management](#).

Features at a Glance

This section provides links to many important features of Ribbon Application Management Platform (RAMP). The **feature list is not** exhaustive. Click a topic to go to the page of interest.

Dashboard

Quickly check the status of devices and performance data collection; and view an alarm summary. Click on the links to launch sections within the application.

RAMP CNF

RAMP Cloud Native Function (CNF) is a fully containerized cloud native solution. The benefits of cloud native applications are, faster time to market, simpler management, cost reduction, automation, and DevOps practices. RAMP CNF includes feature parity with existing hardware or software-based RAMP.

User Management

Create users and assign privileges to control accessing resources. Manage users/user groups and monitor user activity.

Resource Groups

Provide uniform access to a set of devices by placing them in a resource group and associating the resource group with a user group. Use resource groups to define logical partitions of either individual devices or device types.

Local and External Authentication

Performance Management

Collect performance statistics to monitor the health, operational efficiency, and usage levels of devices. Export collected data and set performance thresholds to trigger alarms.

Lawful Intercept

Enable law enforcement agencies to intercept calls and data by configuring a mediation server. Configure SBC/PSX devices with the mediation devices for call data and call content delivery.

Number Portability Services

Configure number portability services with PSX for multiple regions across the world. Enable Local Number Portability (LNP) and Mobile Number Portability (MNP).

Call History

Generate call history reports using CDRs from SBC Core devices.

Network-Wide Provisioning

Provision multiple SBC Core and Edge devices at a time using predefined configurations. Apply homogenous configuration changes, either full or partial.

SBC Backup and Restore

Take a backup of SBC Core and SLB devices. Restore data and applications if the original data and applications are lost or damaged.

Health Reports

Monitor the overall health of the network and devices. Generate health reports with the most vital information to help you reduce downtime.

Inventory Reports

Retrieve hardware and software details from SBC Core and SLB devices. Monitor configuration changes made to a device over a period of time.

Node Lock

Lock devices to prevent users, other than administrators, from accessing the devices. Restrict write access or both read and write access.

User Sessions

Monitor HTTP and SSH user sessions. Terminate user sessions for **system** maintenance or in the event of suspicious user activity.

System Activity Logging

View logs of system activities to troubleshoot network and device issues. Filter and search within system logs.

User Activity Logging

Track all successful and failed login attempts by users. Find the local and external users logged into the system.

Configure multiple authentication methods to access the RAMP GUI. Set up user authentication with the local RAMP database or use external authentication methods (SAML/LDAP).

SBC Upgrade

Upgrade SBC Core, SLB, and SBC Edge devices by uploading installation files.

Call Trace

View call traces initiated on managed SBC Core and GSX devices. Debug policy and call routing issues using call trace information.

Multi-Tenancy

Create distinct entities (tenants) to represent organizations. Use tenants to control access and policies for users and resources.

License Management

Install and activate licenses for devices. Monitor license usage and expiry. Audit license inventory by generating reports.

Fault Management

Identify, isolate, and resolve failures in the network with a highly-customizable interface. Forward, synchronize, and purge alarms.

RAMP CNF - Introduction and Getting Started

In this section:

- [RAMP CNF - Architecture](#)
- [RAMP CNF - System Requirements](#)
- [RAMP CNF - Changes to Existing RAMP Functionalities](#)
- [RAMP CNF - Abbreviations and Terminologies](#)
- [RAMP CNF - Resiliency](#)
 - [RAMP CNF - Geographical Redundancy Configuration](#)
- [RAMP CNF - Observability](#)
- [RAMP CNF - Performance Metrics](#)

Ribbon Application Management Platform (RAMP) is a centralized management client for Ribbon devices in a customer's network.

RAMP provides a complete Fault, Configuration, Accounting, Performance, and Security solution with a portfolio of management and provisioning tools. RAMP provides a range of software and network management functions

for virtualized and cloud-based Ribbon devices. It provides registration services that bring devices into the managed network and offers features to facilitate device configuration and software management.

RAMP Cloud Native Function (CNF) is a fully containerized cloud native solution. The benefits of cloud native applications are, faster time to market, simpler management, cost reduction, automation, and DevOps practices. RAMP CNF includes feature parity with existing hardware or software-based RAMP. You can distribute RAMP CNF users across geographical locations. RAMP CNF provides a northbound REST API for provisioning integration and northbound and southbound SNMPv3 support for trap forwarding.

RAMP CNF - Architecture

In this section:

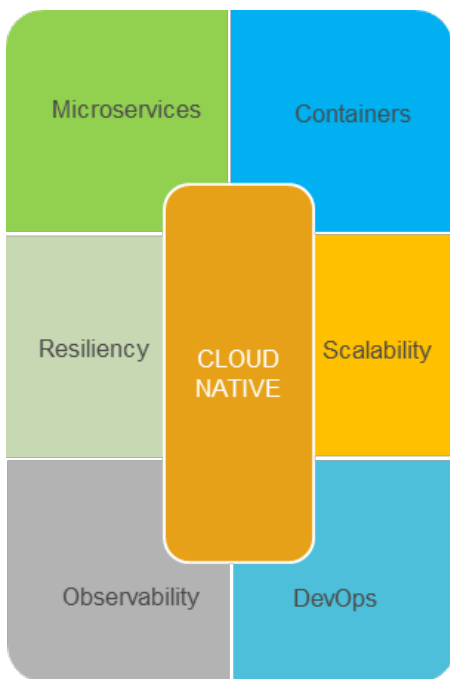
- [Ribbon Cloud Native Overview](#)
 - [Cloud Native Architecture Principles](#)
 - [Ribbon CNF Deployment Model](#)
- [Ribbon CNF Products Architecture](#)
 - [Auto-Scaling](#)
 - [Security](#)
 - [Redundancy](#)
 - [Observability](#)
 - [Application Life Cycle Automation](#)
- [RAMP CNF Architecture](#)

Ribbon Cloud Native Overview

The Ribbon cloud-native Session Border Control solution for the SBC, PSX, and RAMP is a fully containerized cloud-native edition of the respective Ribbon functions. The solution offers all the benefits of cloud-native functions (CNF), including faster time to market, higher scalability, simpler management, reduction in overall cost, and enablement of automation and DevOps practices. The CNF products are the cloud-native decomposition and re-architecture of existing functionality in terms of various loosely coupled microservices that interact to provide the required functionality. This provides the benefits of a cloud-native architecture while meeting the functional objectives and the performance KPIs. You can deploy the CNF products across various container orchestration platforms, including Kubernetes, OpenShift Container Platform (OCP) from Red Hat, and the AWS EKS service. They are also deployed in several customer-specific container platforms.

Cloud Native Architecture Principles

Cloud-native architecture is a software development and deployment approach emphasizing cloud environments' scalability, resilience, and automation.



Some of the basic principles of cloud-native architecture include:

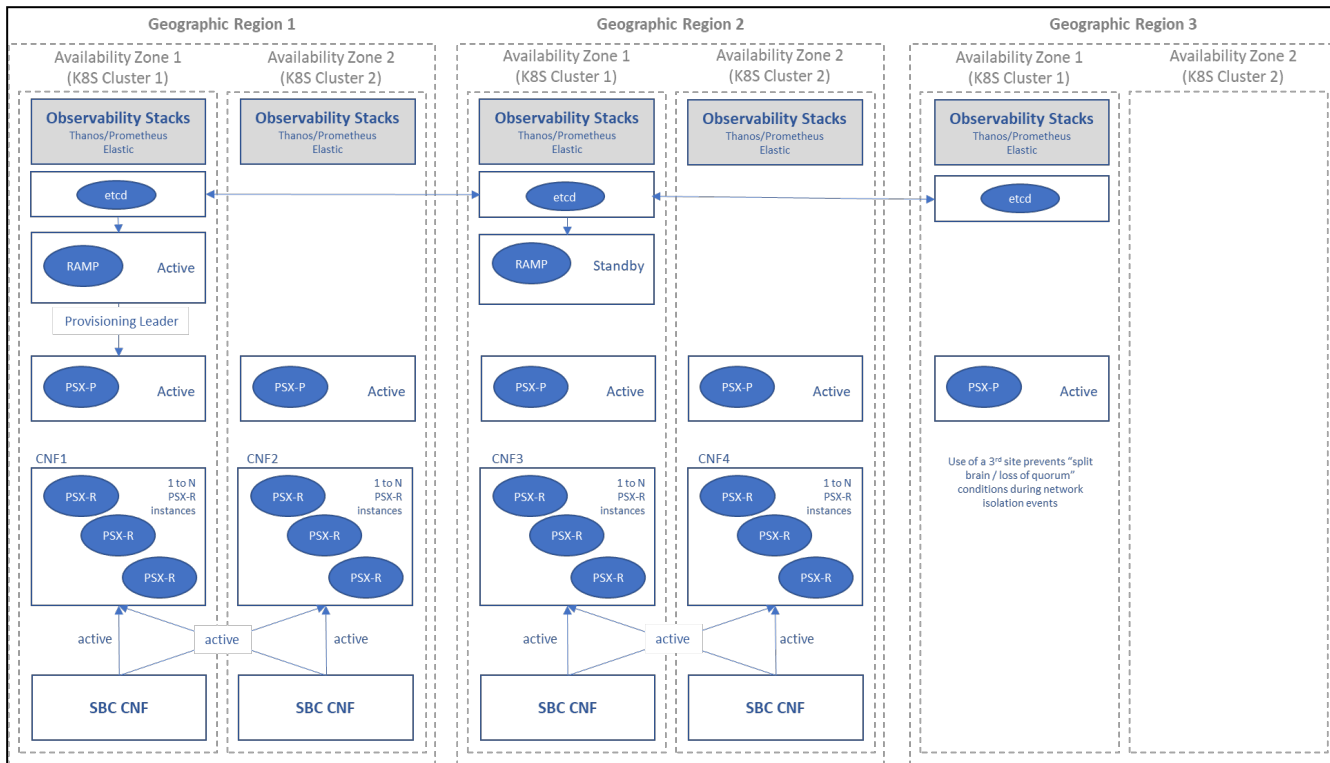
- **Microservices:** The cloud-native architecture emphasizes using small, loosely coupled services developed, deployed, and scaled independently. This approach allows for greater agility and scalability in the application development and deployment process.
- **Containers:** Cloud-native architecture typically relies on containers to package and deploy software applications. Containers provide a lightweight and portable runtime environment deployed across multiple cloud platforms.
- **Resiliency:** Cloud-native applications are designed to be resilient despite failures and disruptions. This includes strategies such as fault tolerance, self-healing, and disaster recovery.
- **Scalability:** Cloud-native architecture emphasizes horizontal scalability, meaning applications can be easily scaled by adding additional instances of the same service.
- **Observability:** Cloud-native applications are designed with observability in mind, providing comprehensive, real-time visibility into the application's performance and behavior.
- **DevOps:** Cloud-native architecture emphasizes a collaborative approach to development and operations, emphasizing automation, Continuous Integration/Continuous Deployment (CI/CD), and rapid iteration.

Ribbon CNF Deployment Model

Ribbon recommends the following model to deploy the Ribbon cloud-native Session Border Control solution in your network:

- **RAMP CNFs** – Always deploy two RAMP CNFs running in Geo-redundancy mode (one RAMP CNF is deployed in a cluster in geographic region/site-1, while the other RAMP CNF is deployed in a cluster in another geographic region/site-2). Dynamically control the state of the RAMP CNFs (i.e., ACTIVE and STANDBY) dynamically using etcd CNFs (3 etcd instances are running in different clusters. Ribbon recommends running the etcd CNFs instances on three distinct geographic regions/sites).
- **PSX-Primary CNFs** – Deploy a minimum of three PSX-Primary CNFs (spread across multiple clusters and geographic regions). When adding additional PSX-Primary CNFs, keep the count odd (primarily to avoid split brain/loss of quorum conditions during network isolation events).
- **PSX-Replica CNFs** – The number of PSX-Replica CNFs to deploy is primarily decided based on the call capacity (i.e., Diameter+ queries, ENUM dips, etc.). Each PSX-Replica CNF will have multiple PSX-Replica pods.

- **SBC CNFs** – The number of SBC CNFs (to achieve cluster level and geographic region/site level redundancy) is decided based on the call pattern (i.e., call/session capacity, call type [passthrough, transcode, direct media], SIPREC, Lawful Intercept, etc). The SC pods in the SBC CNF can dynamically scale up/down based on the call traffic.



Ribbon CNF Products Architecture

The Ribbon CNF architecture is focused on the following five base objectives to achieve cloud-native core capabilities:

1. Auto-Scaling
2. Security
3. Redundancy
4. Observability
5. Application Life Cycle Automation

Auto-Scaling

Auto-scaling is supported for all major Call signaling and media processing pods (Pods are in N:K redundancy model). Auto-scaling is achieved with the Ribbon Horizontal Pod Auto Scaler (RHPA). It does not use the K8S Auto-scaling functionality. The base deployment uses a minimum number of running active and standby pods. If and when the load increases, the RHPA scales out the pods as necessary until reaching the maximum configured number of pods (N+K). Similarly, when the load decreases, the RHPA reduces the number of pods. Currently, only SBC CNe pods have auto-scaling support.

Security

All Ribbon CNF products are deployed in separate namespaces. The SBC CNe is deployed as a separate CNF cluster. The PSX Primary and Replica nodes are deployed as two separate CNF clusters. The SBC CNe and PSX use secure connections to the RAMP.

An inter-pod secure connection is planned in a future release.

Redundancy

All Ribbon CNE products provide Redundancy for their functions (pods). Product-specific (SBC CNE, PSX CNE and RAMP) redundancy mechanisms are explained in their respective product documentation.

Observability

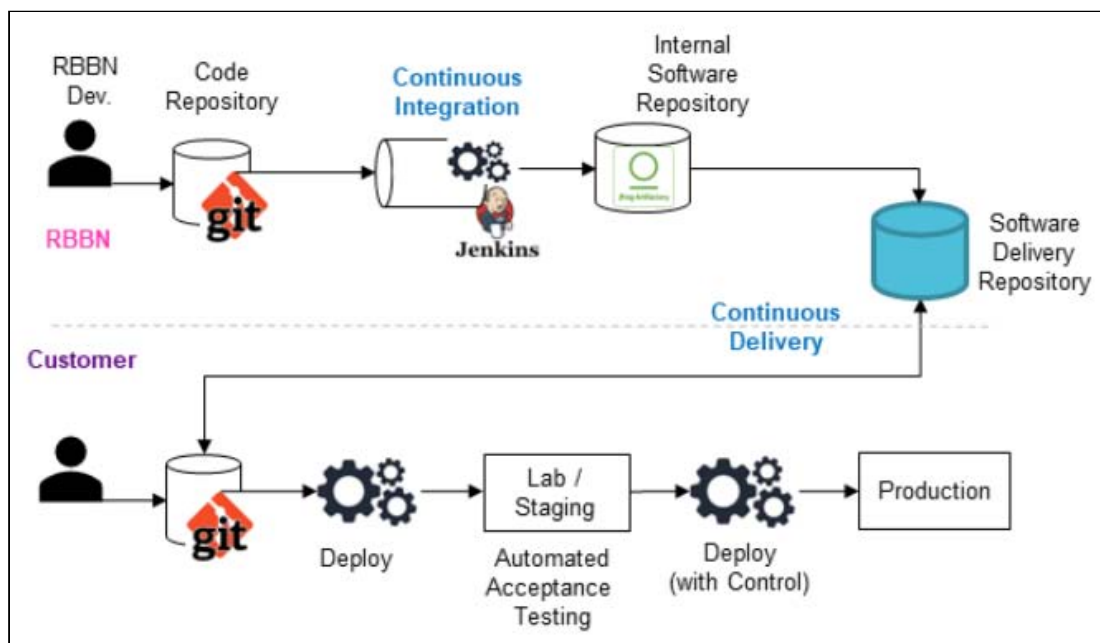
All CNF applications produce logs and metrics that are essential to understanding their state and health. Ribbon CNFs support EFK and Kafka as observability backends for centralized logging, and Prometheus as the metrics logging backend. The interaction with the backends is typically through an integrated telemetry agent in the service pod. Further details are provided later.

Application Life Cycle Automation

The Ribbon CNF Products follow general GitOps principles for life cycle automation. All images are stored in a container repository, and the product manifests (Helm charts) are stored in a Git repository. Any change in the manifests then triggers the pulling of the latest manifests by fluxCD and the modification of the running system parameters to match that of the repository.

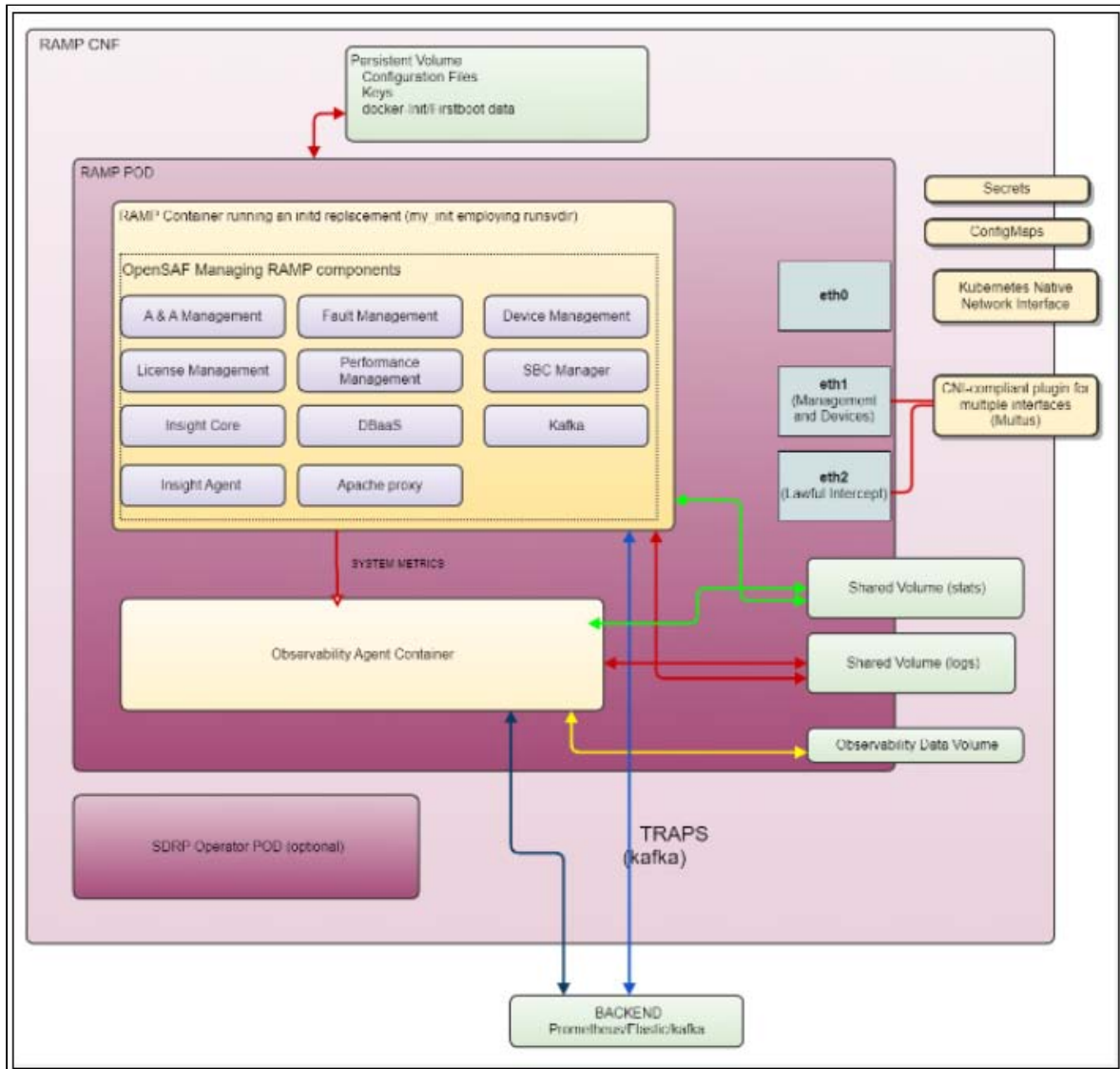
Ribbon customers with appropriate agreements who are eligible to receive new CNF software can obtain the software either by pulling from a Ribbon repository or having it pushed into their repository.

This deployment model assumes the customer is entitled to receive software and artifacts and the interface between the Ribbon and customer's repositories are agreed to and established.



RAMP CNF Architecture

The Ribbon Application Management Platform (RAMP) and Cloud Native Functionality (CNF) functionality provide various microservices that interact with each other to provide the RAMP CNF functionality. The components that makeup RAMP CNF are depicted below.



RAMP CNF - System Requirements

In this section:

- [Hardware Requirements](#)
- [Software Requirements](#)
- [POD and Container Resource Requirements](#)
- [Network Interface Requirements](#)
- [Cluster and Node Level Settings](#)

- [Linux Capabilities](#)
- [Kernel Parameters](#)

The hardware, software, pod, and container requirements for the Ribbon Application Management Platform (RAMP) Cloud Native Functionality (CNF) are provided below.

Hardware Requirements

Processor	For Intel Processors, see the BIOS setting below: <table border="1"> <thead> <tr> <th>BIOS Parameter</th><th>Setting</th></tr> </thead> <tbody> <tr> <td>CPU Power Management Power Regulator</td><td>Maximum performance or Static High Performance</td></tr> <tr> <td>Intel Hyper-Threading</td><td>Enabled</td></tr> <tr> <td>Intel Turbo Boost</td><td>Enabled</td></tr> <tr> <td>Intel VT-x (Virtualization Technology)</td><td>Enabled</td></tr> <tr> <td>Thermal Configuration</td><td>Optimal Cooling or Maximum Cooling</td></tr> <tr> <td>Minimum Processor Idle Power Core C-state</td><td>No C-states</td></tr> <tr> <td>Minimum Processor Idle Power Package C-state</td><td>No C-states</td></tr> <tr> <td>Energy Performance BIAS</td><td>MAX Performance</td></tr> <tr> <td>Sub-NUMA Clustering</td><td>Disabled</td></tr> <tr> <td>HW Prefetcher</td><td>Disabled</td></tr> <tr> <td>Intel® VT-d</td><td>Enabled</td></tr> </tbody> </table>	BIOS Parameter	Setting	CPU Power Management Power Regulator	Maximum performance or Static High Performance	Intel Hyper-Threading	Enabled	Intel Turbo Boost	Enabled	Intel VT-x (Virtualization Technology)	Enabled	Thermal Configuration	Optimal Cooling or Maximum Cooling	Minimum Processor Idle Power Core C-state	No C-states	Minimum Processor Idle Power Package C-state	No C-states	Energy Performance BIAS	MAX Performance	Sub-NUMA Clustering	Disabled	HW Prefetcher	Disabled	Intel® VT-d	Enabled
BIOS Parameter	Setting																								
CPU Power Management Power Regulator	Maximum performance or Static High Performance																								
Intel Hyper-Threading	Enabled																								
Intel Turbo Boost	Enabled																								
Intel VT-x (Virtualization Technology)	Enabled																								
Thermal Configuration	Optimal Cooling or Maximum Cooling																								
Minimum Processor Idle Power Core C-state	No C-states																								
Minimum Processor Idle Power Package C-state	No C-states																								
Energy Performance BIAS	MAX Performance																								
Sub-NUMA Clustering	Disabled																								
HW Prefetcher	Disabled																								
Intel® VT-d	Enabled																								
NIC	Supported NICs: • Intel® Ethernet Network Adapter X710 • Intel® Ethernet Network Adapter X550 • Intel® Ethernet Network Adapter E810 • Mellanox Connectx5 Or Connectx-6																								

Storage	Storage classes: • block • file

Software Requirements

Item	Version/Type	Additional Info
Linux Kernel	4.18 or above	The Linux kernel installed on the worker nodes configured as part of the Kubernetes Cluster.
Kubernetes (K8S)	1.23 or above	N/A
Openshift Container Platform (OCP)	4.8 or above	N/A
Helm	3 or above	N/A
FluxCD	v2 release v0.31.4	Only if GitOps-based installation is performed.

POD and Container Resource Requirements

The following table depicts the system requirements for deploying Kubernetes-based RAMP CNF.

Note

The following PODs and containers are a part of the deployment

POD	Container	vCPU		RAM		H u g e P a g e	E p h e r m a l S t o r a g e	P e r s i s t e n t V o l u m e (P V)	R e p l i c a s
		R e q u e s t	L i m i t	R e q u e s t	L i m i t				

RAMP	RAMP	16	16	64	64	NA	130Gi	450Gi	1
	OBS Agent (RBBN Telemetry)	4	4	8	8			40Gi	1
SDR P Operator (Optional)	Operator	1m	200m	32Mi	512Mi				
	OBS Agent (rbbn-telemetry-agent)	1	1	2Gi	2Gi			20Gi	
	sdr	1m	200m	32Mi	256Mi				

To enable automatic failover on RAMP, you need three additional etcd pods. For etcd resource requirement, refer to [RAMP etcd System Requirements](#).

Network Interface Requirements

Interface	Network Types	Minimum Bandwidth	Additional Information
eth1	macvlan	1 Gbps	northbound and southbound interface

Cluster and Node Level Settings

Configuration Item	Requirement/Usecase	How to check if configured/set/enabled
Multus CNI	RAMP uses non-eth0 interfaces to communicate within northbound and southbound. Multus enables this. Multus CNI plugin enables attaching multiple network interfaces to Pods. Multus acts as a meta-plugin (a CNI plugin that can call multiple other CNI plugins).	<pre>\$kubectl get pods --all- namespaces grep -i multus</pre> Check whether the multus conf file exists <pre>/etc/cni/net.d/00- multus.conf</pre> check multus binary present under <pre>/opt/cni/bin</pre>

Configuration Item	Requirement/Usecase	How to check if configured/set/enabled
Role and Role Binding	Privileges are required to edit/patch/view the resources like endpoint/service (epu for updating the ha0 IP), deployment (hpa, to scale the deployment count), pod (to fetch ha0 IP from annotations), and so forth. Example <pre> apiVersion: rbac.authorization.k8s.io/v1 kind: Role metadata: namespace: {{ .Values.global.namespace }} name: {{ .Release.Name }}-calculator-role rules: - apiGroups: [""] resources: ["pods"] verbs: ["get", "list", "patch", "delete"] - apiGroups: [""] resources: ["pods/log"] verbs: ["get"] - apiGroups: ["rbac.authorization.k8s.io"] resources: ["roles"] verbs: ["get", "list"] - apiGroups: [""] resources: ["endpoints"] verbs: ["get", "list", "patch"] - apiGroups: [""] resources: ["services"] verbs: ["get", "list"] - apiGroups: ["apps"] resources: ["statefulsets"] verbs: ["get", "list"] - apiGroups: ["apps"] resources: ["deployments/scale", "statefulsets/scale"] verbs: ["get", "patch", "update"] - apiGroups: ["apps"] resources: ["deployments"] verbs: ["get", "list", "patch"] - apiGroups: ["metrics.k8s.io"] resources: ["pods"] verbs: ["get", "list"] --- apiVersion: rbac.authorization.k8s.io/v1 kind: RoleBinding metadata: name: {{ .Release.Name }}-calculator-role-binding namespace: {{ .Values.global.namespace }} subjects: - kind: ServiceAccount </pre>	

Configuration Item	Requirement/Usecase	How to check if configured/set/enabled
	<pre> name: {{ .Values.global.serviceAccount.name }} namespace: {{ .Values.global.namespace }} roleRef: kind: Role name: {{ .Release.Name }}-calculator-role apiGroup: rbac.authorization.k8s.io </pre>	
PVC	The RAMP CNF requires the ability to create PVCs in both RWX (ReadWriteMany) and RWO (ReadWriteOnce) modes.	

Linux Capabilities

Capability/securityContext:

- NET_ADMIN
- SYS_RAWIO
- SYS_RESOURCE
- FOWNER
- IPC_LOCK
- KILL
- NET_RAW
- AUDIT_WRITE
- SYS_CHROOT

Kernel Parameters

Parameter	Values
sysctl kernel.pid_max	>= 4096
fs.inotify.max_user_instances	8192

RAMP CNF - Changes to Existing RAMP Functionalities

In this section:

- [Traps](#)
- [Statistics](#)
- [Logs](#)

This section details the changes to existing functionalities of the Ribbon Application Management Platform (RAMP) Cloud Native Functionality (CNF).

Traps

- In a RAMP CNF deployment, SNMP traps are forwarded in `json` format to the Kafka topic.
- The RAMP CNF forwards traps using the ETSI_SOL003 (`json`) format to the Kafka topic. Do not change these values in the `Helm` chart.
- All the traps received by the RAMP CNF are forwarded to the Kafka topic if the required configuration is provided as described in the Helm chart description.
- Traps received from non-CNF devices specify "NA" in the container and pod details for `json` file formatted traps.
- Each trap is assigned a unique id (in the "id" field of the `json` output) based on the source. Each time the trap is received from the same source (root object), the RAMP CNF uses the previously-created id and increments its count by 1 until the trap clears.
- Upon receiving a "clear" trap, the RAMP CNF sets the "id" of the previously-received problem trap in the "id" field of this clear trap while forwarding it.

Here is a sample of the Kafka exported trap details:

Example

```
{
  "rootCause": false,
  "id": "98",
  "managedObjectId": "bnknsccpscpk101",
  "cnf_uuid": "bnknsccpscpk101",
  "cnfc_uuid": "bnknsccpscpk101-oam",
  "ns_uuid": "nsbnknsccpscpk101",
  "podName": "rampsvtjenkinssbc1-oam-7dd8b6db8c-ttbx5",
  "containerName": "oam-container",
  "nodeName": "worker-11.blr-ocp3.lab.rbbn.com",
  "alarmRaisedTime": "2024-11-12T11:11:09+05:30",
  "alarmChangedTime": "2024-11-12T17:40:33+05:30",
  "ackState": "UNACKNOWLEDGED",
  "perceivedSeverity": "WARNING",
  "eventTime": "2024-11-12T17:40:33+05:30",
  "eventType": "QOS_ALARM",
  "probableCause": "lossOfRedundancy",
  "rootObject": "NA",
  "isRootCause": false,
  "faultDetails": "The current event file logging state for log type packet is on.
Node id: 10011 Event log state: 2 Event log type: 7",
  "faultName": "sonusCpEventLogFileStateNotificationCnf"
}
```

Statistics

- The RAMP CNF also collects statistics from all devices with statistics collection enabled. The only difference is that resource usage statistics are no longer collected for the RAMP container by the PM.

- The PM profiles for GSX, SGX, and DSI are configured with an additional export location (`/opt/rbbn/rbbn-telemetry/pm_stats/input`) in addition to the default location. The files exported to `/opt/rbbn/rbbn-telemetry/pm_stats/input` are read by the OBS agent since it is a shared volume. The OBS agent exposes these stats for scraping at regular intervals.
- By default, the "**all node export**" option is enabled in PM. It is recommended to use the "**per profile export**" option, to ensure only the required statistics are shared with the OBS agent. The OBS agent expects the files in the `.tar.gz` format. If the export mode is "**Per node export**" then the OBS does not parse and forward it to the backend server.
- The OBS agent uses the configuration provided in the Helm chart (`pm_stats_demo.yaml`) for parsing all the statistics. Currently, it is configured to parse statistics of the GSX, SGX, and DSI as other CNF devices expose their own interfaces through the OBS agent for scraping the PM data.
- A Maximum of 10,000 metrics are exported to Prometheus.

Logs

- All the logs generated by the RAMP CNF are parsed by the OBS agent and exported to elasticSearch/ Kafka in the `json` file format.
- The regex patterns for parsing the logs present in the RAMP CNF are present in `ramp_parser.conf` file packaged along with the RAMP Helm chart.

RAMP CNF - Abbreviations and Terminologies

This page lists the terminologies and abbreviations used in the Ribbon Application Management Platform (RAMP) Cloud Native Functionality (CNF) sections.

Common CNF Terms

Term	Ribbon Definitions / Usage
Container	A Container image is a ready-to-run software package, containing everything needed to run a function: the code and any runtime it requires, application and system libraries, and default values for any essential settings. By design, a container is immutable: you cannot change the code of a container that is already running. If you have a containerized function and want to make changes, you must build a new image that includes the change, then recreate the container to start from the updated image.
Database shard	Database sharding splits a single dataset into partitions (or shards). Each shard contains unique rows of information that you can store separately across multiple nodes. All shards run on separate nodes but share the original database's schema or design.
K8S ConfigMap	A ConfigMap is an API object that allows you to store data as key-value pairs. Kubernetes pods can use ConfigMaps as configuration files, environment variables or command-line arguments. ConfigMaps allow you to decouple environment-specific configurations from containers to make applications portable. For details, refer to https://kubernetes.io/docs/concepts/configuration/configmap/

Term	Ribbon Definitions / Usage
K8S Daemonset	DaemonSet feature is used to ensure that some or all of your pods are scheduled and running on every single available node in the K8S cluster. This essentially runs a copy of the desired pod across all nodes. When a new node is added to a Kubernetes cluster, a new pod is added to that newly attached node. For details, refer to https://kubernetes.io/docs/concepts/workloads/controllers/daemonset/
K8S Deployment	A Deployment is a resource object in Kubernetes that provides declarative updates to applications. A deployment allows you to describe an application's life cycle, such as which images to use for the app, the number of required pods and the pod update method. For details, refer to https://kubernetes.io/docs/concepts/workloads/controllers/deployment/
K8S Job	A Job is a supervisor for pods carrying out batch processes, that is, a process that runs for a certain time to completion. For details, refer to https://kubernetes.io/docs/concepts/workloads/controllers/job/
K8S Persistent Volume (PV)	A PersistentVolume is a piece of storage in the cluster that has been provisioned by an administrator or dynamically provisioned using Storage Classes. PVs are volume plugins like Volumes but have a lifecycle independent of any individual pod that uses the PV. GlusterFS is used in the Ribbon VNF to share the data across managed nodes. Some use cases for PV include: • The configurations are shared from OAM across other pods via PV • Performance statistics are shared from various pods to OAM via PV
K8S Persistent Volume Claim (PVC)	A PersistentVolumeClaim is a request for storage by a user. It is similar to a pod. Pods consume node resources and PVCs consume PV resources. Pods can request specific levels of resources (CPU and Memory). Claims can request specific size and access modes (e.g., mounted as ReadWriteOnce, ReadOnlyMany or ReadWriteMany). For details, refer to https://kubernetes.io/docs/concepts/storage/persistent-volumes/
K8S pod	A pod is the smallest deployable units of computing that you can create and manage in Kubernetes. A pod is a group of one or more container with shared storage and network resources and a specification for how to run the containers. Additional information: • Pod – https://kubernetes.io/docs/concepts/workloads/pods/ • Deployment – https://kubernetes.io/docs/concepts/workloads/controllers/deployment/
K8S Replicaset	A ReplicaSet is a process that runs multiple instances of a pod and keeps the specified number of pods constant. Its purpose is to maintain the specified number of pod instances running in a cluster at any given time to prevent users from losing access to their application when a pod fails or is inaccessible. For details, refer to https://kubernetes.io/docs/concepts/workloads/controllers/replicaset/

Term	Ribbon Definitions / Usage
K8S Rollout	Rollout simply means rolling update of application. Rolling update means that application is updated gradually, gracefully and with no downtime. For details, refer to https://argoproj.github.io/argo-rollouts/
K8S Secrets	A Secret is an object that contains a small amount of sensitive data such as a password, a token, or a key. Such information might otherwise be put in a pod specification or in a container image. Using a Secret means that you don't need to include confidential data in your application code. For details, refer to https://kubernetes.io/docs/concepts/configuration/secret/
K8S Service	A Service is a logical abstraction for a deployed group of pods in a cluster (which all perform the same function). Since pods are ephemeral, a service enables a group of pods, which provide specific functions (web services, image processing, etc.) to be assigned a name and unique IP address (clusterIP). For details, refer to https://kubernetes.io/docs/concepts/services-networking/service/
K8S Statefulset	A StatefulSet is the workload API object used to manage stateful applications. Manages the deployment and scaling of a set of pods, and provides guarantees about the ordering and uniqueness of these pods. For details, refer to https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/
K8S Storage Class (SC)	A StorageClass provides a way for administrators to describe the "classes" of storage they offer. Different classes might map to quality-of-service levels, or to backup policies, or to arbitrary policies determined by the cluster administrators. For details, refer to https://kubernetes.io/docs/concepts/storage/storage-classes/
Microservice	Microservices – also known as the microservice architecture - is an architectural style that structures an application as a collection of services that are: • Highly maintainable and testable • Loosely coupled • Independently deployable • Organized around business capabilities • Owned by a small team
Observability	Observability – A complex system's internal state can be deduced from external outputs. The goal of Ribbon observability is to facilitate the exposure of metrics and logs. Ribbon uses OpenTelemetry to implement the Ribbon Observability Stack and supports the selected components from the OpenTelemetry community. Ribbon's aim is to support all CNF-based Ribbon products in order to stream the observability data. With the introduction of this new stack, all logs and metrics and in future traces are normalized and pre-processed, which will help to correlate multiple data points captured from each microservice and deliver them to configured backends.
RBBN Application	An Application (or Application Service for aaS offers) is composed of one or more CNFs. In the near term an Application will likely map 1:1 with a CNF (eg: SBC CNF).

Term	Ribbon Definitions / Usage
RBBN CNF	A Cloud-Native Network Function is a software-implementation of a Network Function implemented in container(s) and orchestrated by Kubernetes, built and deployed in a cloud-native way. A CNF is a single deployable, upgradable and manageable entity. – A RBBN CNF consists or 1 or more pods, packaged via a Helm Chart.
RBBN CNF Solution Hierarchy	• Solution → Collection of Helm Charts ◦ Application (1-n...) → currently 1:1, Application to CNF • Pod (1-n...) ◦ Container (1-n...)
RBBN Solution	A RBBN Solution consists of a collection of Applications or CNFs which together form an overall solution (e.g., a solution may contain RAMP, PSX, AS and SBC Applications). The scope of the application teams is to define LCM operations, and the Solutions/Services teams define the solution with workflows integrating application level LCM operations. Note: Ribbon Call Trust and Ribbon Voice Sync are examples of Solutions composed of multiple Applications/CNFs.

Abbreviations Used in CNF Documentation

Abbreviation	Definition
AA	Authentication and Authorization
CAC	Call Admission Control
CI/CD	Continuous Integration/Continuous Deployment
CM	Configuration Management
CNCF	Cloud Native Computing Foundation
CNe	Cloud-Native edition
CNF	Cloud Native Network Function
CS	Common Services
DBaaS	DB as a Service
DevOps	Development and Operations
DM	Device Management

Abbreviation	Definition
EFK	Elasticsearch, Fluentd, and Kibana stack
EPU	Endpoint Updater
FCAPS	Faults, Configuration, Accounting, Performance, and Security
FM	Fault Management
FR	Fixed Resource
	Modified: for 12.1.4
HPA	Horizontal Pod Autoscaler
IDM	Identity Management
K8S	Kubernetes
LM	License Management
NS	Network Services
OAM	Operations, Administration and Maintenance
OC	OpenShift CLI
OCP	OpenShift Container Platform
PM	Performance Metrics
PSX-P	PSX Primary
PSX-R	PSX Replica
RAC	Role Assignment Controller
RBBN	Ribbon Communications
RHPA	Ribbon Horizontal Pod Autoscaler
SC	Session Control

Abbreviation	Definition
SIP-T	SIP-Telephony
SLB	SIP Load Balancer
TOSCA	Topology and Orchestration Specification for Cloud Applications

RAMP CNF - Resiliency

In this section:

- [RAMP CNF - Geographical Redundancy Configuration](#)
 - [RAMP CNF - Set up an etcd Cluster](#)
 - [Deploying RAMP with existing secret](#)
 - [Enabling SSL for Kafka Forwarder](#)
 - [Deploying etcd with Existing Secret](#)
 - [RAMP CNF - Set up an etcd Cluster on Private Cloud](#)

Related article:

[Generate Redundancy Templates](#)

Cloud native applications include strategies for resiliency such as fault tolerance, self-healing, and disaster recovery to protect against disruptions and failures.

RAMP CNF - Geographical Redundancy Configuration

In this section:

- [RAMP CNF - Set up an etcd Cluster](#)
 - [Deploying RAMP with existing secret](#)
 - [Enabling SSL for Kafka Forwarder](#)
 - [Deploying etcd with Existing Secret](#)
- [RAMP CNF - Set up an etcd Cluster on Private Cloud](#)

Related articles:

- [Managing Redundancy](#)
- [Generate Redundancy Templates](#)
- [Configuring RAMP GR with Automatic Switchover Enabled](#)

Use the following procedure to configure a Geographically Redundant (GR) Ribbon Application Management Platform (RAMP) deployment. Generate a redundancy template file before running the procedure to specify the deployment's configuration details. For more information, refer to [Generate Redundancy Templates](#).

Run the procedure on the RAMP device that you designate as the source/active node for the GR deployment. It is not necessary to repeat the setup on the target/standby device.

RAMP GR is supported in KVM, VMware, CNF, and OpenStack environments.

Note

The following procedure describes configuring a standard GR deployment in which switchovers are triggered manually. RAMP also supports a deployment model that enables automatic switchover between GR instances. To enable automatic switchover, you must deploy three additional VMs, each running an instance of etcd. You also specify different redundancy template parameters to enable automatic switchover. For more information, refer to [Configuring RAMP GR with Automatic Switchover Enabled](#).

Prerequisites

- Two RAMP devices are up and running in the same environment with the same version.
- For RAMP on CNF, the two RAMP devices are running on separate OpenShift Container Platforms (OCP).
- The Standby device is accessible from the active device, and vice versa.

Note

If you restored the database on an OpenStack deployment, password-less SSH from the Active RAMP device to the Standby RAMP device (and vice versa) is not possible until GR is configured.

- Verify if you can ping the Standby device from the Active device and you can ping the Active device from the Standby device.
- The same password is set for the `admin` and `insight` users on the Active and Standby devices.

Note

The `insight` password is reset in the RAMP Active device after restoring the database (with the password of the old database).

- If you manually create `cron` entries on the RAMP Active device, you must also create the same `cron` entries on the Standby device. In RAMP GR, `cron` entries are not copied and synchronized from Active to Standby, or vice versa.
- Ensure that the network and prefix of the Standby RAMP is provided in the Helm chart of the Active RAMP. This ensures that the Active RAMP adds the route since it uses eth1 for communication.
- Likewise, ensure the network and prefix of the Active RAMP is provided in the Helm chart of Standby RAMP.
- Generate the redundancy template file for the deployment. For more information, refer to [Generate Redundancy Templates](#).
- Before you run the `RDsetup.sh` command, set the session timeout interval to zero (0) by performing the procedure at [Modify User Session Timeout Interval](#). After you modify the session timeout interval, re-initiate a new SSH session and then run the `RDsetup.sh` command.

Start

1. Log on to the RAMP CLI as an `admin` user to establish it as the source/active node in the GR deployment.
2. Change to the `root` user:

```
sudo su -
```

- Specify the path and name of the redundancy template file generated for your GR deployment:

```
/etc/sonus/RDsetup.sh <absolute path to the redundancy template file>
```

Example specifying a redundancy template file, GR.conf, in the /opt directory:

```
/etc/sonus/RDsetup.sh /opt/GR.conf
```

Example output:

```
[16:17:41] Starting redundancy cluster setup .....
[16:17:42]
Building RD configuration locally .....
Please enter Password of admin user for all nodes (press ENTER if not needed) ->
admin
```

- Enter the `admin` password.

Note

If you are configuring a GR deployment on OpenStack and the password-less authentication is enabled for the `admin` user from the active RAMP device to the Standby RAMP device, press **ENTER**.

The script completes the GR setup, and the RAMP process starts shortly.

- Check Active RAMP status. For more information, refer to [Check RAMP Status](#).
- Check Standby RAMP status. For more information, refer to [Check RAMP Status](#).

Note

For a RAMP CNF deployment:

- The readiness probe runs only on the Active RAMP indicating that its container is ready to accept traffic.
- There is a warning on the Standby RAMP indicating that the readiness probe is not running.

- Restore the session timeout interval to 750 by performing the procedure at [Modify User Session Timeout Interval](#).

Resume or Restart Setup

If the configuration process is interrupted and you resume `RDsetup.sh`, RAMP prompts you with a confirmation message:

```
Record showing the <script name> script was being executed and was not completed.
Do you want to resume the operation from the previous point of failure (yes|no)?.
```

Choose an option:

- Enter "yes" to resume the operation from the point of failure.
- Enter "no" to restart the script. A confirmation message displays:

```
Do you want to proceed with a fresh new operation (yes|no)? ->
```

Choose an option:

- Enter "yes" to run the script.
- Enter "no" to terminate the session.

RAMP CNF - Set up an etcd Cluster

In this section:

- [Overview](#)
- [Set up etcd on RAMP CNF](#)
- [View Etcd Member List](#)
 - [CNF etcd Status](#)
 - [etcd Health Status](#)

Related articles:

- [Configuring RAMP GR with Automatic Switchover Enabled](#)
- [Deployment Models](#)
- [RAMP Security Group Rules](#)
- [Configuring RAMP Redundancy](#)
- [Setting Up an etcd Cluster](#)
- [Managing Redundancy](#)

Overview

Three etcd VMs are required to monitor a Ribbon Access Management Platform (RAMP) Geographically Redundant (GR) deployment for automatic switchover. Refer to [Configuring RAMP GR with Automatic Switchover Enabled](#) for information on how the etcd VMs are involved in the GR deployment.

You can instantiate these VMs on VMware, KVM, or OpenStack. However, you are not required to deploy the etcd VMs on the same platform as the RAMP instances. Use the following procedure to set up etcd on RAMP CNF.

Set up etcd on RAMP CNF

Prerequisites

- Three free IP addresses are available to allocate to the etcd instances.
- The recommended configuration is 1 vCPU and 2GB of memory.
- 1 Gi etcd container for 500 Mi observability center.

- 2 Gi etcd container for 1 Gi observability center.
- Ensure the platforms use RCP 5.4.3 and/or OCP RH-openshift 4.10.18 or later versions.

Start

1. Log onto the Ribbon Support portal and download the Helm chart for etcd. Refer to [Download Files from Ribbon Support Portal](#) for information on using the portal.
2. Untar the Helm chart:

```
tar -xvf <name of the Helm chart>.tar
```

3. Change the directory:

```
cd etcd/
```

4. Edit the values in the `yaml` file:

```
vi values.yml
```

Parameters

Parameters To Edit	Description	Example	Notes
imageCredentials	Credentials to artifactory.	<pre> global: imageCredentials: name: "" registry: "xxxxxx" username: "xxxxx" password: "xxxx" obs-common-modules: imageCredentials: # Specifies whether an image credentials secret should be created create: true ## @param imageRegistryPath Containers image repository path in the registry ## imageRegistryPath: "/" dockerhub-docker-remote" image: repository: bitnami/etcd tag: 3.5.7 ## Specify a imagePullPolicy ## Defaults to 'Always' if image tag is 'latest', else set to 'IfNotPresent' ## ref: https:// kubernetes.io/docs/user- guide/images/#pre-pulling- images ## pullPolicy: IfNotPresent </pre>	Leave the name field empty. Provide the registry from where the image is located. Under obs-common-modules, set create as "true" for "imageCredentials". Provide the imageRegistryPath and the pull policy. To see policy values, refer to https://kubernetes.io/docs/user-guide/images/#pre-pulling-images.
cluster name	Provide a name for the etcd cluster.	clusterName: "etcdctl1"	

Parameters To Edit	Description	Example	Notes
<code>existingEndpoints</code>	current endpoints available in cluster (IP/FQDN)	IP: <code>existingEndpoints: "http://172.29.208.33:30082"</code> FQDN : <code>existingEndpoints: "http://worker-10.blr-cp1.lab.rbbn.com:30082"</code>	Parameter is not needed while creating the first etcd instance. It is only mandatory for the second and third etcd instances. For example, <code>existingEndpoints: "http://172.29.208.33:30082, http://172.29.208.34:30083"</code> .
<code>initialCluster</code>	Initial cluster configuration for bootstrap.	<code>initialCluster: ""</code>	If the existing endpoints are specified, this parameter is ignored.
<code>initialClusterState</code>	The initial state when a cluster is being created. Values are either 'new' or 'existing'.	<code>initialClusterState="new"</code>	If these values are not set, then set the following default values: ◦ <code>'new'</code> - while installing the chart ('<code>helm install ...</code>') ◦ <code>'existing'</code> - while upgrading the chart ('<code>helm upgrade</code> ') or while "<code>existingEndpoints</code>" are set.

Parameters To Edit	Description	Example	Notes
service	NodePort / clusterIP / LoadBalancer	NODEPORT : <pre> service: type: "NodePort" enabled: true ###ports in range 30000 - 32000 for host port nodePorts: client: "" peer: "" LoadBalancer : service: type: "LoadBalancer " enabled: true loadBalancerIP: "xx.xx.xx.xx" ## @param service.ports.client etcd client port ## @param service.ports.peer etcd peer port ## ports: client: 2379 peer: 2380 </pre>	By default, the ports are selected randomly. If you set the ports manually, then select the NodePort: ◦ The host port range is 30000 - 32000 ◦ When Loadbalancer is added as Service, the Service type is "Loadbalancer". ◦ Provide the Loadbalancer IP address. ◦ The default ports for loadbalancer are "2379" and "2380".

Parameters To Edit	Description	Example	Notes
Certificates	a. CertManager b. Client and Server certificates	<pre>certManager: enabled: true issuer: name: "<Name of Issuer>" kind: "<Issuer kind>" auth: client: secureTransport: true enableAuthentication: true certDuration: "" server: secureTransport: true enableAuthentication: true certDuration: ""</pre>	◦ Enable CertManager. ◦ Provide the Issuer type and name. ◦ If you are using NodePort with TLS, set the <code>certExtraDnsSans</code> parameters with the worker node name. ◦ In values.yaml under auth, enable secureTransport and enableAuthentication as true ◦ You can also provide the duration of expiry of certificate. The Client section provides information on the tls communication between endpoint, etcd, and server section among the etcds in a cluster. The client and server certificates use the port "2379". The client certificate is used for <code>etcdctl</code>.

Parameters To Edit	Description	Example	Notes
volume obs	logPersistentVolume Storage	<pre># Storage request limit for PVC logPersistentVolumeStorage: # Specifies whether a # service account should be # created for the observability # components create: true</pre>	Enable logPersistentVolumeStorage for creating pvc for etcd.
Role	Roles for SA.	<pre>roles: ## @param roles.create ## Enable/disable Role and ## RoleBinding creation. If set ## to false, the ServiceAccount ## passed in global will need ## the following rules: ## If using a NodePort ## service: ## - apiGroups: [""] # "" ## indicates the core API ## group ## resources: ## ["services"] ## verbs: ["get"] ## If using persistence: ## - apiGroups: [""] ## resources: ## ["persistentvolumeclaims"] ## verbs: ["get", "list", ## "delete", "deletecollection"] ## ## create: true</pre>	Set this to "true" so you can delete/uninstall pvc.

5. Install the Helm chart after editing the values in the `values.yaml` file:

```
helm install <deployment name> -f values.yaml .
```

A sample of the `values.yaml`

Example of the values.yaml file

```
## @section Global parameters
```

```

## Please, note that this will override the image parameters, including
dependencies, configured to use the global value
##
global:
  ## @param global.imageRegistry Containers image registry
  ##
  imageRegistry: "artifactory-tx.rbbn.com"
  ## @param global.imagePullSecrets [array] Global Docker registry secret names
as an array
  ## E.g.
  ## imagePullSecrets:
  ##   - name: myRegistryKeySecretName
  ## Note: for backwards compatibility, directly specifying the secrets as a
list of strings without the name: attribute is also supported, but not
recommended
  ##
  imagePullSecrets: ["etcd-imagecred"]
  ## @param global.imagePullSecretsTemplate [array]
  ## Template strings to evaluate to existing secret to use to pull images, for
example: name: "{.Release.Name }-imagecred"
  ##
  imagePullSecretsTemplate: []
  ## @param imageCredentials Create image pull credentials
  ##
  imageCredentials:
    name: "etcd-rco"
    registry: artifactory-tx.rbbn.com
    username: ssequeira
    password: xxxxxxxxxx
  ## @param global.serviceAccount to use for pods
  ##
  serviceAccount:
    ## @param global.serviceAccount.name Name of the service account to use
    ##
    name: ""
  ## @param global.storageClass Global StorageClass for Persistent Volume(s)
  ##
  storageClass: ""
  ## Cert-manager information to use in the csi-driver volume
  ##
  certManager:
    ## @param global.certManager.enabled Switch to enable the use of cert-
manager to manage certificates
    ##
    enabled: true
    issuer:
      ## @param global.certManager.issuer.name The Issuer name to sign the
certificate request
      ##
      name: "cross-cluster-ca-selfsigned-clusterissuer"
      ## @param global.certManager.issuer.kind The Issuer kind to sign the
certificate request. Can be "Issuer" or "ClusterIssuer"

```

```

    ## See https://cert-manager.io/docs/concepts/issuer/ for more information
    ##
    kind: "ClusterIssuer"
  ## @param global.ns_uuid Global NS UUID
  ##
  ns_uuid: ""
  ## @param global.cnf_uuid Global CNF UUID
  ##
  cnf_uuid: ""
  ## @param global.cnfc_uuid Global CNFC UUID
  ##
  cnfc_uuid: ""
  ## @param global.obs parameters
  ##
  ## @param global.kubernetesPlatform K8s platform type: "oc" or "robin"
  ##
  kubernetesPlatform: ""
  obs:
    ## @param global.obs.image image parameters
    ##
    image:
      ## @param global.obs.image.repository observability agent image name
      ##
      repository: "ccs-docker-prod-virtual/rbbn_telemetry_collector"
      ## @param global.obs.image.tag observability agent image tag
      ##
      tag: "3.0.2"
      ## @param global.obs.image.pullPolicy observability agent image pull
      ## policy. Defaults to 'Always' if image tag is 'latest', else set to
      ## 'IfNotPresent'
      pullPolicy: IfNotPresent
    ## @param global.obs.logPersistentVolumeStorage settings for log PVC
    ##
    logPersistentVolumeStorage:
      ## @param global.obs.logPersistentVolumeStorage.request Size of the PVC
      ## storage request
      ##
      request: 20Gi
    ## @param global.obs.logs parameters
    ##
    logs:
      ## @param global.obs.logs.telemetry log telemetry config
      ## telemetry:
      ## @param global.obs.logs.telemetry.topic telemetry logs will be sent
      ## to this Kafka topic
      ##
      topic: rbbn-otel-agent
      ## @param global.obs.logs.backendServers log backends
      ##
      backendServers: {}
      ## @param obs.logs.backendServers.elasticsearch elasticsearch backend

```



```

    ## Warning: username and password represent the name of the ENV variable
name
    ## that contains the username and password from the secret
    # elasticsearch:
    #   - endpoint: <elasticsearch server address>:443
    #   auth: True
    #   username: ELASTICSEARCH_USER
    #   password: ELASTICSEARCH_PASSWD
    #   index: <filebeat index>
    ## @param obs.logs.backendServers.kafka kafka backend
    ##
    # kafka:
    #   - endpoint: <kafka server address>:<kafka port>
    #   sslCert: KAFKA_CERT
    #   sslKey: KAFKA_KEY
    #   sslCa: KAFKA_CA
    ## @param global.obs.logs.elasticsearchSecretName name of common
elasticsearch credentials secret
    ##
    elasticsearchSecretName: ""
    ## @param obs.logs.kafkaSecretName Name of secret containing Kafka
environment variables
    ## Evaluated as a template, for example: "{{ .Release.Name }}-
elasticsearch-user-creds"
    #
    elasticsearchSecretNameTemplate: ""
    ## @param global.obs.logs.elasticsearchSecretName name of common kafka
credentials secret
    ##
    kafkaSecretName: ""
    ## @param obs.global.logs.kafkaSecretName Name of secret containing Kafka
environment variables
    ## Evaluated as a template, for example: "{{ .Release.Name }}-kafka-user-
creds"
    ##
    kafkaSecretNameTemplate: ""

    ## @param global.prometheusRule Prometheus alerting rules
    ##
    prometheusRule:
    ## @param global.prometheusRule.create Specifies whether a PrometheusRule
resource should be created
    ##
    # create: false
    ## @param global.prometheusRule.labels Specify additional labels so the
Prometheus instance can discover the rules
    ##
    labels: {}

    ## @param global.customizedResourcePrefix template definitions for resource
name prefixes
    ##

```

```

customizedResourcePrefix:
  servicePrefixTemplate: ""
  configmapPrefixTemplate: ""

persistence:
  ## @param global.persistence.annotations Annotations to add to the
  PersistentVolumeClaims
  ##
  annotations: {}

## @section Common parameters

## @param kubeVersion Force target Kubernetes version (using Helm capabilities
if not set)
##
kubeVersion: ""
## @param nameOverride String to partially override etcd.fullname template
(will maintain the release name)
##
nameOverride: ""
## @param fullnameOverride String to fully override etcd.fullname template
##
fullnameOverride: ""
## @param commonLabels [object] Labels to add to all deployed objects
##
commonLabels: {}
## @param commonAnnotations [object] Annotations to add to all deployed objects
##
commonAnnotations: {}
## @param clusterDomain Default Kubernetes cluster domain
##
clusterDomain: cluster.local
## @param extraDeploy [array] Array of extra objects to deploy with the release
##
extraDeploy: []

## @section roles parameters
##
roles:
  ## @param roles.create Enable/disable Role and RoleBinding creation. If set
  to false, the ServiceAccount passed in global will need the following rules:
  ## If using a NodePort service:
  ## - apiGroups: ["" ] # "" indicates the core API group
  ##   resources: ["services"]
  ##   verbs: ["get"]
  ## If using persistence:
  ## - apiGroups: ["" ]
  ##   resources: ["persistentvolumeclaims"]
  ##   verbs: ["get", "list", "delete", "deletecollection"]
  ##
  create: false

```

```

## Enable diagnostic mode in the deployment
##
diagnosticMode:
  ## @param diagnosticMode.enabled Enable diagnostic mode (all probes will be
  disabled and the command will be overridden)
  ##
  enabled: false
  ## @param diagnosticMode.command [array] Command to override all containers
  in the deployment
  ##
  command:
    - sleep
  ## @param diagnosticMode.args [array] Args to override all containers in the
  deployment
  ##
  args:
    - infinity

## @param imageRegistryPath Containers image repository path in the registry
##
imageRegistryPath: "/dockerhub-docker-remote"

## @section etcd parameters

## etcd image version
## ref: https://console.cloud.google.com/gcr/images/etcd-development/GLOBAL/etcd
## ref: https://hub.docker.com/r/bitnami/etcd/tags/
## @param image.repository etcd image name
## @param image.tag etcd image tag
## @param image.pullPolicy etcd image pull policy
##
image:
  repository: bitnami/etcd
  tag: 3.5.11
  ## Specify a imagePullPolicy
  ## Defaults to 'Always' if image tag is 'latest', else set to 'IfNotPresent'
  ## ref: https://kubernetes.io/docs/user-guide/images/#pre-pulling-images
  ##
  pullPolicy: IfNotPresent
  ## Set to true if you would like to see extra information on logs
  ##
  debug: false
## kubectl image (used for init and cleanup)
## ref: https://hub.docker.com/r/bitnami/kubectl/tags/
## @param kubectl.image.repository kubectl image name
## @param kubectl.image.tag kubectl image tag
##
kubectl:
  image:
    repository: bitnami/kubectl
    tag: 1.26.2

```

```

## Authentication parameters
##
auth:
  ## Role-based access control parameters
  ## ref: https://etcd.io/docs/current/op-guide/authentication/
  ##
  rbac:
    ## @param auth.rbac.create Switch to enable RBAC authentication
    ##
    create: false
    ## @param auth.rbac.allowNoneAuthentication Allow to use etcd without
    configuring RBAC authentication
    ##
    allowNoneAuthentication: true
    ## @param auth.rbac.rootPassword Root user password. The root user is
    always `root`
    ##
    rootPassword: ""
    ## @param auth.rbac.existingSecret Name of the existing secret containing
    credentials for the root user
    ##
    existingSecret: ""
    ## @param auth.rbac.existingSecretPasswordKey Name of key containing
    password to be retrieved from the existing secret
    ##
    existingSecretPasswordKey: ""
  ## Authentication token
  ## ref: https://etcd.io/docs/latest/learning/design-auth-v3/#two-types-of-tokens-simple-and-jwt
  ##
  token:
    ## @param auth.token.type Authentication token type. Allowed values:
    'simple' or 'jwt'
    ## ref: https://etcd.io/docs/latest/op-guide/configuration/#--auth-token
    ##
    type: jwt
    ## @param auth.token.privateKey.filename Name of the file containing the
    private key for signing the JWT token
    ## @param auth.token.privateKey.existingSecret Name of the existing secret
    containing the private key for signing the JWT token
    ## NOTE: Ignored if auth.token.type=simple
    ## NOTE: A secret containing a private key will be auto-generated if an
    existing one is not provided.
    ##
    privateKey:
      filename: jwt-token.pem
      existingSecret: ""
    ## @param auth.token.signMethod JWT token sign method
    ## NOTE: Ignored if auth.token.type=simple
    ##
    signMethod: RS256
    ## @param auth.token.ttl JWT token TTL

```

```

    ## NOTE: Ignored if auth.token.type=simple
    ##
    ttl: 10m
    ## TLS authentication for client-to-server communications
    ## ref: https://etcd.io/docs/current/op-guide/security/
    ##
    client:
      ## @param auth.client.secureTransport Switch to encrypt client-to-server
communications using TLS certificates
      ##
      secureTransport: true
      ## @param auth.client.useAutoTLS Switch to automatically create the TLS
certificates
      ##
      useAutoTLS: false
      ## @param auth.client.existingSecret Name of the existing secret containing
the TLS certificates for client-to-server communications
      ##
      existingSecret: ""
      ## @param auth.client.enableAuthentication Switch to enable host
authentication using TLS certificates. Requires existing secret
      ##
      enableAuthentication: true
      ## @param auth.client.certFilename Name of the file containing the client
certificate
      ##
      certFilename: cert.pem
      ## @param auth.client.certKeyFilename Name of the file containing the
client certificate private key
      ##
      certKeyFilename: key.pem
      ## @param auth.client.caFilename Name of the file containing the client CA
certificate
      ## If not specified and `auth.client.enableAuthentication=true` or
`auth.rbac.enabled=true`, the default is is `ca.crt`
      ##
      caFilename: "ca.pem"
      ## @param auth.client.certDuration Requested duration the signed
certificate will be valid for
      ##
      certDuration: ""
      ## @param auth.client.certExtraDnsSans DNS Subject Alternative Name to add
to the certificates
      ##
      certExtraDnsSans: ""
      ## @param auth.client.certExtraIpSans IP Subject Alternative Name to add to
the certificates
      ##
      certExtraIpSans: ""
    ## TLS authentication for server-to-server communications
    ## ref: https://etcd.io/docs/current/op-guide/security/
    ##

```

```

peer:
  ## @param auth.peer.secureTransport Switch to encrypt server-to-server
communications using TLS certificates
  ##
  secureTransport: true
  ## @param auth.peer.useAutoTLS Switch to automatically create the TLS
certificates
  ##
  useAutoTLS: false
  ## @param auth.peer.existingSecret Name of the existing secret containing
the TLS certificates for server-to-server communications
  ##
  existingSecret: ""
  ## @param auth.peer.enableAuthentication Switch to enable host
authentication using TLS certificates. Requires existing secret
  ##
  enableAuthentication: true
  ## @param auth.peer.certFilename Name of the file containing the peer
certificate
  ##
  certFilename: cert.pem
  ## @param auth.peer.certKeyFilename Name of the file containing the peer
certificate private key
  ##
  certKeyFilename: key.pem
  ## @param auth.peer.caFilename Name of the file containing the peer CA
certificate
  ## If not specified and `auth.peer.enableAuthentication=true` or
`rbac.enabled=true`, the default is is `ca.crt`
  ##
  caFilename: "ca.pem"
  ## @param auth.peer.certDuration Requested duration the signed certificate
will be valid for
  ##
  certDuration: ""
  ## @param auth.peer.certExtraDnsSans DNS Subject Alternative Name to add to
the certificates
  ##
  certExtraDnsSans: ""
  ## @param auth.peer.certExtraIpSans IP Subject Alternative Name to add to
the certificates
  ##
  certExtraIpSans: ""
  ## @param autoCompactionMode Auto compaction mode, by default periodic. Valid
values: "periodic", "revision".
  ## - 'periodic' for duration based retention, defaulting to hours if no time
unit is provided (e.g. 5m).
  ## - 'revision' for revision number based retention.
  ##
  autoCompactionMode: ""
  ## @param autoCompactionRetention Auto compaction retention for mvcc key value
store in hour, by default 0, means disabled

```

```

##
autoCompactionRetention: ""
## @param heartbeatInterval Cluster leader heartbeat interval, in ms (by
default 100)
## Refer to https://etcd.io/docs/v3.5/tuning/#time-parameters
##
heartbeatInterval: ""
## @param electionTimeout Timeout after which a follower will start an election
when not receiving a leader heartbeat, in ms (by default 1000)
## Refer to https://etcd.io/docs/v3.5/tuning/#time-parameters
##
electionTimeout: ""
## @param clusterName Cluster name - this is the name of the etcd cluster.
##
clusterName: "etcd"
## @param existingEndpoints Existing cluster endpoints to use for
bootstrapping.
## When this is set, the etcd instance created by this chart will add itself as
a member of the cluster.
## An example is: "https://etcd1:2379,https://etcd2:2379"
##
existingEndpoints: ""
## @param initialCluster Initial cluster configuration for bootstrapping.
## When existingEndpoints is specified, this parameter is ignored.
## If existingEndpoints and this parameter are not specified, etcd will default
to "default=http://localhost:2380"
## An example is: "etcd1=https://etcd1:2380,etcd2=https://
etcd2:2380,etcd3=https://etcd3:2380"
##
initialCluster: ""
## @param initialClusterState Initial cluster state. Allowed values: 'new' or
'existing'.
## If this values is not set, the default values below are set:
## - 'new': when installing the chart ('helm install ...')
## - 'existing': when upgrading the chart ('helm upgrade ...') or when
existingEndpoints is set
##
initialClusterState: ""
## @param discoverySrv DNS SRV domain used to bootstrap the cluster.
## ref: https://etcd.io/docs/v3.5/op-guide/clustering/#dns-discovery
##
discoverySrv: ""
## @param discoverySrvName Suffix to the DNS SRV name queried when
bootstrapping using DNS.
## ref: https://etcd.io/docs/v3.5/op-guide/clustering/#dns-discovery
##
discoverySrvName: ""
## @param memberCount Number of etcd member(s) to deploy. Maximum value: 3.
## WARNING: This parameter MUST NOT be modified during an upgrade. Modifying
this value will cause the etcd member(s) to be restarted,
## potentially causing an unrecoverable loss of quorum.
##

```

```

memberCount: 1
## @param maxProcs Limits the number of operating system threads that can
execute user-level
## Go code simultaneously by setting GOMAXPROCS environment variable
## ref: https://golang.org/pkg/runtime
##
maxProcs: ""
## @param removeMemberOnUninstall Use a pre-delete chart hook to remove the
etcd member from the etcd cluster on chart uninstall
##
removeMemberOnUninstall: true
## @param configuration etcd configuration. Specify content for etcd.conf.yml
## e.g:
## configuration: |-
##     foo: bar
##     baz:
##
configuration: ""
## @param existingConfigmap Existing ConfigMap with etcd configuration
## NOTE: When it's set the configuration parameter is ignored
##
existingConfigmap: ""
## @param extraEnvVars [array] Extra environment variables to be set on etcd
container
## e.g:
## extraEnvVars:
##   - name: F00
##     value: "bar"
##
extraEnvVars: []
## @param extraEnvVarsCM Name of existing ConfigMap containing extra env vars
##
extraEnvVarsCM: ""
## @param extraEnvVarsSecret Name of existing Secret containing extra env vars
##
extraEnvVarsSecret: ""
## @param command [array] Default container command (useful when using custom
images)
##
command: []
## @param args [array] Default container args (useful when using custom images)
##
args: []

## @section etcd statefulset parameters

statefulset:
  ## @param statefulset.enabled create statefulset if equal true
  ##
  enabled: true

## Update strategy

```



```

## ref: https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/
#update-strategies
## @param updateStrategy.type Update strategy type, can be set to RollingUpdate
or OnDelete.
##
updateStrategy:
  type: RollingUpdate
## @param podManagementPolicy Pod management policy for the etcd statefulset
## ref: https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/
#pod-management-policies
##
podManagementPolicy: Parallel
## @param hostAliases [array] etcd pod host aliases
## ref: https://kubernetes.io/docs/concepts/services-networking/add-entries-to-
pod-etc-hosts-with-host-aliases/
##
hostAliases: []
## @param lifecycleHooks [object] Override default etcd container hooks
##
lifecycleHooks: {}
## etcd container ports to open
## @param containerPorts.client Client port to expose at container level
## @param containerPorts.peer Peer port to expose at container level
##
containerPorts:
  client: 2379
  peer: 2380
## etcd pods' Security Context
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/security-
context/#set-the-security-context-for-a-pod
## @param podSecurityContext.enabled Enabled etcd pods' Security Context
## @param podSecurityContext.fsGroup Set etcd pod's Security Context fsGroup
##
podSecurityContext:
  enabled: true
  fsGroup: 1001
## etcd containers' SecurityContext
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/security-
context/#set-the-security-context-for-a-container
## @param containerSecurityContext.enabled Enabled etcd containers' Security
Context
## @param containerSecurityContext.runAsUser Set etcd container's Security
Context runAsUser
## @param containerSecurityContext.runAsNonRoot Set etcd container's Security
Context runAsNonRoot
##
containerSecurityContext:
  enabled: true
  runAsUser: 1001
  runAsNonRoot: true
## etcd containers' resource requests and limits
## ref: https://kubernetes.io/docs/user-guide/compute-resources/

```

```

## We usually recommend not to specify default resources and to leave this as a
conscious
## choice for the user. This also increases chances charts run on environments
with little
## resources, such as Minikube. If you do want to specify resources, uncomment
the following
## lines, adjust them as necessary, and remove the curly braces after
'resources:'.
## @param resources.limits [object] The resources limits for the etcd container
## @param resources.requests [object] The requested resources for the etcd
container
##
resources:
  limits:
    cpu: 1
    memory: 2Gi
  requests:
    cpu: 1m
    memory: 128Mi
## Configure extra options for liveness probe
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/#configure-probes
## @param livenessProbe.enabled Enable livenessProbe
## @param livenessProbe.initialDelaySeconds Initial delay seconds for
livenessProbe
## @param livenessProbe.periodSeconds Period seconds for livenessProbe
## @param livenessProbe.timeoutSeconds Timeout seconds for livenessProbe
## @param livenessProbe.failureThreshold Failure threshold for livenessProbe
## @param livenessProbe.successThreshold Success threshold for livenessProbe
##
livenessProbe:
  enabled: true
  initialDelaySeconds: 300
  periodSeconds: 30
  timeoutSeconds: 5
  successThreshold: 1
  failureThreshold: 5
## Configure extra options for readiness probe
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/#configure-probes
## @param readinessProbe.enabled Enable readinessProbe
## @param readinessProbe.initialDelaySeconds Initial delay seconds for
readinessProbe
## @param readinessProbe.periodSeconds Period seconds for readinessProbe
## @param readinessProbe.timeoutSeconds Timeout seconds for readinessProbe
## @param readinessProbe.failureThreshold Failure threshold for readinessProbe
## @param readinessProbe.successThreshold Success threshold for readinessProbe
##
## BE CAREFUL!!! If using a Service, traffic will not be sent to the Pods until
they are Ready.
## This can lead to a deadlock where the etcd members cannot communicate and
start the cluster.

```

```

##
readinessProbe:
  enabled: false
  initialDelaySeconds: 10
  periodSeconds: 10
  timeoutSeconds: 5
  successThreshold: 1
  failureThreshold: 5
## Configure extra options for liveness probe
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/#configure-probes
## @param startupProbe.enabled Enable startupProbe
## @param startupProbe.initialDelaySeconds Initial delay seconds for
  startupProbe
## @param startupProbe.periodSeconds Period seconds for startupProbe
## @param startupProbe.timeoutSeconds Timeout seconds for startupProbe
## @param startupProbe.failureThreshold Failure threshold for startupProbe
## @param startupProbe.successThreshold Success threshold for startupProbe
##
startupProbe:
  enabled: false
  initialDelaySeconds: 0
  periodSeconds: 10
  timeoutSeconds: 5
  successThreshold: 1
  failureThreshold: 60
## @param customLivenessProbe [object] Override default liveness probe
##
customLivenessProbe: {}
## @param customReadinessProbe [object] Override default readiness probe
##
customReadinessProbe: {}
## @param customStartupProbe [object] Override default startup probe
##
customStartupProbe: {}
## @param extraVolumes [array] Optionally specify extra list of additional
  volumes for etcd pods
##
extraVolumes: []
## @param extraVolumeMounts [array] Optionally specify extra list of additional
  volumeMounts for etcd container(s)
##
extraVolumeMounts: []
## @param initContainers [array] Add additional init containers to the etcd
  pods
## e.g:
## initContainers:
##   - name: your-image-name
##     image: your-image
##     imagePullPolicy: Always
##     ports:
##       - name: portname

```

```

##          containerPort: 1234
##
initContainers: []
## @param sidecars [array] Add additional sidecar containers to the etcd pods
## e.g:
## sidecars:
##   - name: your-image-name
##     image: your-image
##     imagePullPolicy: Always
##     ports:
##       - name: portname
##         containerPort: 1234
##
sidecars: []
## @param podAnnotations [object] Annotations for etcd pods
## ref: https://kubernetes.io/docs/concepts/overview/working-with-objects/annotations/
##
podAnnotations: {}
## @param podLabels [object] Extra labels for etcd pods
## Ref: https://kubernetes.io/docs/concepts/overview/working-with-objects/labels/
##
podLabels: {}
## @param podLabelsTemplate [object] Extra labels for etcd pods that can
## contain variables
##
podLabelsTemplate: {}
## @param affinity [object] Affinity for pod assignment
## Ref: https://kubernetes.io/docs/concepts/configuration/assign-pod-node/#affinity-and-anti-affinity
##
affinity: {}
## @param nodeSelector [object] Node labels for pod assignment
## Ref: https://kubernetes.io/docs/user-guide/node-selection/
##
nodeSelector: {}
## @param tolerations [array] Tolerations for pod assignment
## Ref: https://kubernetes.io/docs/concepts/configuration/taint-and-toleration/
##
tolerations: []
## @param terminationGracePeriodSeconds Seconds the pod needs to gracefully
## terminate
## ref: https://kubernetes.io/docs/concepts/containers/container-lifecycle-hooks/#hook-handler-execution
##
terminationGracePeriodSeconds: ""
## @param schedulerName Name of the k8s scheduler (other than default)
## ref: https://kubernetes.io/docs/tasks/administer-cluster/configure-multiple-schedulers/
##
schedulerName: ""

```

```

## @param priorityClassName Name of the priority class to be used by etcd pods
## Priority class needs to be created beforehand
## Ref: https://kubernetes.io/docs/concepts/configuration/pod-priority-preemption/
##
priorityClassName: ""
## @param topologySpreadConstraints Topology Spread Constraints for pod
assignment
## https://kubernetes.io/docs/concepts/workloads/pods/pod-topology-spread-constraints/
## The value is evaluated as a template
##
topologySpreadConstraints: []

## @section Service exposing the etcd member outside the Kubernetes cluster

service:
  ## @param service.type Kubernetes Service type. Supported value: "NodePort"
  and "LoadBalancer"
  ## Note: There is always a headless service enabled to expose the etcd member
  within the Kubernetes cluster
  ##
  type: ""
  ## @param service.enabled create service to expose etcd outside a Kubernetes
  cluster in combination with sdrp-operator if equal true
  ##
  enabled: false
  ## @param service.dualStack exposes the service on both IPv4 and IPv6 if
  available when set to true
  ##
  dualStack: false
  ## @param service.clusterIP Kubernetes service Cluster IP
  ## e.g.:
  ## clusterIP: None
  ##
  clusterIP: ""
  ## @param service.ports.client etcd client port
  ## @param service.ports.peer etcd peer port
  ##
  ports:
    client: 2379
    peer: 2380
  ## @param service.nodePorts.client Specify the nodePort client value for the
  LoadBalancer and NodePort service types.
  ## @param service.nodePorts.peer Specify the nodePort peer value for the
  LoadBalancer and NodePort service types.
  ## ref: https://kubernetes.io/docs/concepts/services-networking/service/
  #type-nodeport
  ##
  nodePorts:
    client: ""
    peer: ""

```

```

    ## @param service.loadBalancerIP loadBalancerIP for the etcd service
(optional, cloud specific)
    ## ref: https://kubernetes.io/docs/user-guide/services/#type-loadbalancer
    ##
    loadBalancerIP: ""
    ## @param service.loadBalancerSourceRanges [array] Load Balancer source
ranges
    ## ref: https://kubernetes.io/docs/tasks/access-application-cluster/
configure-cloud-provider-firewall/#restrict-access-for-loadbalancer-service
    ## e.g:
    ## loadBalancerSourceRanges:
    ##   - 10.10.10.0/24
    ##
    loadBalancerSourceRanges: []
    ## @param service.externalIPs [array] External IPs
    ## ref: https://kubernetes.io/docs/concepts/services-networking/service/
#external-ips
    ##
    externalIPs: []
    ## @param service.externalTrafficPolicy %%MAIN_CONTAINER_NAME%% service
external traffic policy
    ## ref http://kubernetes.io/docs/tasks/access-application-cluster/create-
external-load-balancer/#preserving-the-client-source-ip
    ##
    externalTrafficPolicy: Cluster
    ## @param service.extraPorts Extra ports to expose (normally used with the
`sidecar` value)
    ##
    extraPorts: []
    ## @param service.labels [object] Additional labels for the etcd service
    ##
    labels: {}
    ## @param service.annotations [object] Additional annotations for the etcd
service
    ##
    annotations: {}
    ## @param service.sessionAffinity Session Affinity for Kubernetes service,
can be "None" or "ClientIP"
    ## If "ClientIP", consecutive client requests will be directed to the same
Pod
    ## ref: https://kubernetes.io/docs/concepts/services-networking/service/
#virtual-ips-and-service-proxies
    ##
    sessionAffinity: None
    ## @param service.sessionAffinityConfig Additional settings for the
sessionAffinity
    ## sessionAffinityConfig:
    ##   clientIP:
    ##     timeoutSeconds: 300
    ##
    sessionAffinityConfig: {}

```

```

    ## @param service.sdrpScope When using sdrp-operator, this is the scope where
    the SRV record is published.
    ## The A/AAAA record will always be published in the cluster scope.
    ## Allowed value: "global" or "cluster"
    ## Depending on this value, also configure "sdrpClusterDomain" or
    "sdrpGlobalDomain" to enable automation
    ## of the configuration of the peer urls of this member with the fqdn of this
    service published by sdrp-operator.
    ##
    sdrpScope: "global"
    ## @param service.sdrpClusterDomain Cluster domain where the service is
    published when using sdrp-operator
    ## This allow generating a fqdn representing the service globally.
    ## Required to allow geo-distributed etcd cluster when using a service of
    type "LoadBalancer".
    ##
    sdrpClusterDomain: ""
    ## @param service.sdrpGlobalDomain Global domain where the service is
    published when using sdrp-operator
    ## This allow generating a fqdn representing the service globally.
    ##
    sdrpGlobalDomain: ""
    ## @param service.sdrpClientFqdnInstance Overrides the instance part of the
    FQDN for the etcd client SRV record published for the service.
    ## When it is used: <k8s service name>._<type>._<protocol>.<domain> ->
    <instance>._<type>._<protocol>.<domain>
    ## Fill this with the same in every Helm release when deploying multiple
    instances of this chart (i.e. multicluster)
    ## to publish SRV records for all instances under the same FQDN
    sdrpClientFqdnInstance: ""
    ## @param service.extraFqdns [array] Extra fqdn(s) representing this service
    ## When cert-manager is generating certificates, this fqdn(s) will be added
    in the certificate SAN.
    ## This fqdn(s) will also be added to the etcd member advertised url(s). The
    fqdn(s) MUST be resolvable,
    ## otherwise, the etcd member will be unusable.
    ## NOTE: When using a service of type "LoadBalancer" and not using the sdrp-
    operator, this allow providing
    ## a fqdn representing the load balancer.
    ## NOTE: When using a service of type "NodePort", this allow providing
    node(s) fqdn. You will need to manually
    ## update the etcd member to add the peer urls based on this fqdn(s) once a
    port is assigned.
    ##
    extraFqdns: []

## @section networkInterface
## Using pod network interface for etcd communications
## When using TLS it is mandatory to either provide static ip or configure sdrp
operator
## For using sdrp operator, the interface, sdrpScope and sdrpClusterDomain
values should be provided

```

```

## For using static ip, the ip value should be defined
##
networkInterface:
  ## @param networkInterface.name selected network interface information for
  etcd communication
  ## Etcd will be exposed through the selected network interface
  ## It should be chosen according to the name defined in networkAnnotation in
  the networkAnnotations section
  ## To enable using the network interface the name of available network should
  be provided
  ##
  name: 'ext-static-net-1-ipv6'
  ## @param networkInterface.interface This is the name of interface that etcd
  will be exposed through.
  ## This variable should be provided when using sdrp operator
  ##
  interface: ''
  ## @param networkInterface.ip The ip that etcd will be exposed through.
  ## This variable should be specified when using static ip deployment
  ##
  ip: 'fd2c:4708:5563:1511::341'
  ## @param networkInterface.addressIndex Index of IP address to use from
  attached network
  ## For example, can be used for selecting an IPv6 address on a dual-stack
  network
  ##
  addressIndex: 0
  ## @param networkInterface.defaultRoute This is the optional variable that
  will be provided to k8s.v1.cni.cncf.io/networks annotation of pod
  ## It will be assigned to the "default-route" of k8s.v1.cni.cncf.io/networks
  annotation
  ##
  defaultRoute: 'fd2c:4708:5563:1511::301'
  ## @param networkInterface.namespace This is the optional variable that will
  be provided to k8s.v1.cni.cncf.io/networks annotation of pod
  ## It will be assigned to the "namespace" of k8s.v1.cni.cncf.io/networks
  annotation
  ##
  namespace: ''
  ## @param networkInterface.sdrpScope When using sdrp-operator, this is the
  scope where the SRV record is published.
  ## The A/AAAA record will always be published in the cluster scope.
  ## Allowed value: "global" or "cluster"
  sdrpScope: ''
  ## @param networkInterface.sdrpClusterDomain domain where the network
  interface is published when using sdrp-operator in the scope
  ## This allow generating a fqdn representing the network interface in the
  scope.
  ## this is the variable that shows to use the sdrp.
  sdrpClusterDomain: ''
  ## @param service.sdrpClientFqdnInstance Overrides the instance part of the
  FQDN for the etcd client SRV record published for the service.

```



```

    ## When it is used: <k8s service name>._<type>._<protocol>.<domain> ->
    <instance>._<type>._<protocol>.<domain>
    ## Fill this with the same in every Helm release when deploying multiple
    instances of this chart (i.e. multicluster)
    ## to publish SRV records for all instances under the same FQDN
    sdrpClientFqdnInstance: ''

## @section Persistence parameters

## Enable persistence using Persistent Volume Claims
## ref: https://kubernetes.io/docs/user-guide/persistent-volumes/
##
persistence:
    ## @param persistence.enabled If true, use a Persistent Volume Claim. If
false, use emptyDir.
    ##
    enabled: true
    ## @param persistence.storageClass Persistent Volume Storage Class
    ## If defined, storageClassName: <storageClass>
    ## If set to "-", storageClassName: "", which disables dynamic provisioning
    ## If undefined (the default) or set to null, no storageClassName spec is
    ## set, choosing the default provisioner. (gp2 on AWS, standard on
    ## GKE, AWS & OpenStack)
    ##
    storageClass: ""
    ##
    ## @param persistence.annotations [object] Annotations for the PVC
    ##
    annotations: {}
    ## @param persistence.accessModes Persistent Volume Access Modes
    ##
    accessModes:
        - ReadWriteOnce
    ## @param persistence.size PVC Storage Request for etcd data volume
    ##
    size: 1Gi
    ## @param persistence.selector [object] Selector to match an existing
    Persistent Volume
    ## ref: https://kubernetes.io/docs/concepts/storage/persistent-volumes/
#selector
    ##
    selector: {}

## @section Volume Permissions parameters

## Init containers parameters:
## volumePermissions: Change the owner and group of the persistent volume
mountpoint to runAsUser:fsGroup values from the securityContext section.
##
volumePermissions:
    ## @param volumePermissions.enabled Enable init container that changes the
    owner and group of the persistent volume(s) mountpoint to `runAsUser:fsGroup`

```

```

##
enabled: false
## @param volumePermissions.image.repository Init container volume-
permissions image name
## @param volumePermissions.image.tag Init container volume-permissions image
tag
## @param volumePermissions.image.pullPolicy Init container volume-
permissions image pull policy
##
image:
  repository: bitnami/bitnami-shell
  tag: 10-debian-10-r387
  pullPolicy: IfNotPresent
## Init container' resource requests and limits
## ref: https://kubernetes.io/docs/user-guide/compute-resources/
## We usually recommend not to specify default resources and to leave this as
a conscious
## choice for the user. This also increases chances charts run on
environments with little
## resources, such as Minikube. If you do want to specify resources,
uncomment the following
## lines, adjust them as necessary, and remove the curly braces after
'resources:'.
## @param volumePermissions.resources.limits [object] Init container volume-
permissions resource limits
## @param volumePermissions.resources.requests [object] Init container
volume-permissions resource requests
##
resources:
  ## Example:
  ## limits:
  ##   cpu: 500m
  ##   memory: 1Gi
  limits: {}
  requests: {}

## @section Network Policy parameters
## ref: https://kubernetes.io/docs/concepts/services-networking/network-
policies/
##
networkPolicy:
  ## @param networkPolicy.enabled Enable creation of NetworkPolicy resources
  ##
  enabled: false
  ## @param networkPolicy.allowExternal Don't require client label for
connections
  ## When set to false, only pods with the correct client label will have
network access to the ports
  ## etcd is listening on. When true, etcd will accept connections from any
source
  ## (with the correct destination port).
  ##

```

```

allowExternal: true
## @param networkPolicy.extraIngress [array] Add extra ingress rules to the
NetworkPolicy
## e.g:
## extraIngress:
##   - ports:
##     - port: 1234
##     from:
##       - podSelector:
##         - matchLabels:
##           - role: frontend
##       - podSelector:
##         - matchExpressions:
##           - key: role
##             operator: In
##             values:
##               - frontend
##
extraIngress: []
## @param networkPolicy.extraEgress [array] Add extra ingress rules to the
NetworkPolicy
## e.g:
## extraEgress:
##   - ports:
##     - port: 1234
##     to:
##       - podSelector:
##         - matchLabels:
##           - role: frontend
##       - podSelector:
##         - matchExpressions:
##           - key: role
##             operator: In
##             values:
##               - frontend
##
extraEgress: []
## @param networkPolicy.ingressNSMatchLabels [object] Labels to match to
allow traffic from other namespaces
## @param networkPolicy.ingressNSPodMatchLabels [object] Pod labels to match
to allow traffic from other namespaces
##
ingressNSMatchLabels: {}
ingressNSPodMatchLabels: {}

## @section Snapshotting parameters

## Start a new etcd cluster recovering the data from an existing snapshot
before bootstrapping
##
startFromSnapshot:

```

```

    ## @param startFromSnapshot.enabled Initialize new cluster recovering an
existing snapshot
    ##
    enabled: false
    ## @param startFromSnapshot.existingClaim Existing PVC containing the etcd
snapshot
    ##
    existingClaim: ""
    ## @param startFromSnapshot.snapshotFilename Snapshot filename
    ##
    snapshotFilename: ""
## Enable auto disaster recovery by periodically snapshotting the keyspace:
## - It creates a cronjob to periodically snapshotting the keyspace
## - It also creates a ReadWriteMany PVC to store the snapshots
##
disasterRecovery:
    ## @param disasterRecovery.enabled Enable auto disaster recovery by
periodically snapshotting the keyspace
    ##
    enabled: false
    cronjob:
        ## @param disasterRecovery.cronjob.schedule Schedule in Cron format to save
snapshots
        ## See https://en.wikipedia.org/wiki/Cron
        ##
        schedule: "*/30 * * * *"
        ## @param disasterRecovery.cronjob.historyLimit Number of successful
finished jobs to retain
        ##
        historyLimit: 1
        ## @param disasterRecovery.cronjob.snapshotHistoryLimit Number of etcd
snapshots to retain, tagged by date
        ##
        snapshotHistoryLimit: 1
        ## @param disasterRecovery.cronjob.podAnnotations [object] Pod annotations
for cronjob pods
        ## ref: https://kubernetes.io/docs/concepts/overview/working-with-objects/
annotations/
        ##
        podAnnotations: {}
        ## Configure resource requests and limits for snapshotter containers
        ## ref: https://kubernetes.io/docs/user-guide/compute-resources/
        ## We usually recommend not to specify default resources and to leave this
as a conscious
        ## choice for the user. This also increases chances charts run on
environments with little
        ## resources, such as Minikube. If you do want to specify resources,
uncomment the following
        ## lines, adjust them as necessary, and remove the curly braces after
'resources:'.
        ## @param disasterRecovery.cronjob.resources.limits [object] Cronjob
container resource limits

```

```

    ## @param disasterRecovery.cronjob.resources.requests [object] Cronjob
container resource requests
    ##
    resources:
      limits:
        cpu: 500m
        memory: 1Gi
      requests:
        cpu: 1m
        memory: 64Mi
    ## @param disasterRecovery.cronjob.nodeSelector Node labels for cronjob
pods assignment
    ## Ref: https://kubernetes.io/docs/user-guide/node-selection/
    ##
    nodeSelector: {}
    ## @param disasterRecovery.cronjob.tolerations Tolerations for cronjob pods
assignment
    ## Ref: https://kubernetes.io/docs/concepts/configuration/taint-and-toleration/
    ##
    tolerations: []

pvc:
    ## @param disasterRecovery.pvc.existingClaim A manually managed Persistent
Volume and Claim
    ## If defined, PVC must be created manually before volume will be bound
    ## The value is evaluated as a template, so, for example, the name can
depend on .Release or .Chart
    ##
    existingClaim: ""
    ## @param disasterRecovery.pvc.size PVC Storage Request
    ##
    size: 1Gi
    ## @param disasterRecovery.pvc.storageClassName Storage Class for snapshots
volume
    ##
    storageClassName: managed-nfs-storage

## @section Service account parameters

serviceAccount:
    ## @param serviceAccount.create Enable/disable service account creation
    ##
    create: false
    ## @param serviceAccount.name Name of the service account to create or use
    ##
    name: ""
    ## @param serviceAccount.automountServiceAccountToken Enable/disable auto
mounting of service account token
    ## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/#use-the-default-service-account-to-access-the-api-server
    ##

```

```

    automountServiceAccountToken: true
    ## @param serviceAccount.annotations [object] Additional annotations to be
    included on the service account
    ##
    annotations: {}
    ## @param serviceAccount.labels [object] Additional labels to be included on
    the service account
    ##
    labels: {}

## @section Other parameters

## etcd Pod Disruption Budget configuration
## ref: https://kubernetes.io/docs/tasks/run-application/configure-pdb/
##
pdb:
    ## @param pdb.create Enable/disable a Pod Disruption Budget creation
    ##
    create: false
    ## @param pdb.minAvailable Minimum number/percentage of pods that should
    remain scheduled
    ##
    minAvailable: 1
    ## @param pdb.maxUnavailable Maximum number/percentage of pods that may be
    made unavailable
    ##
    maxUnavailable: ""

## @section Security parameters for service mesh
##
security:
    ## @param security.create Enable/disable service mesh security creation
    ##
    create: false
    ## @param security.allowPlaintextClient Switch to disable plaintext client.
    When false, client must have tls enabled
    ##
    allowPlaintextClient: false
    ## @param security.allowedClientNamespaces [array] List of namespaces that
    can use a client to talk to the etcd cluster
    ##
    allowedClientNamespaces: []
    ## @param security.allowedMemberNamespaces [array] List of namespaces that
    can have an etcd member in the cluster
    ##
    allowedMemberNamespaces: []

## @section Routing parameters for service mesh
##
routing:
    ## @param routing.create Enable/disable service mesh gateway creation for
    etcd

```

```

##
create: false
## @param routing.enabled Enable/disable service mesh virtual service routing
creation for etcd
##
enabled: false
## ingress gateway ports to use for etcd
## @param routing.ingressGatewayPorts.client Client port to use at gateway
level
## @param routing.ingressGatewayPorts.peer Peer port to use at gateway level
##
ingressGatewayPorts:
  client: 2379
  peer: 2380
## @param routing.allowedIpBlocks [array] List of single IP or CIDR that can
use a client to talk to the etcd cluster or have an etcd member in the cluster
##
allowedIpBlocks: []

## @section Prometheus Rule
##
prometheusRule:
  ## @param prometheusRule.create Specifies whether a PrometheusRule resource
should be created (alerting rule definitions)
  ##
  # create: false
  ## @param prometheusRule.labels Specify additional labels so the Prometheus
instance can discover the rules
  ##
  labels: {}

## @section Observability agent
##
obs:
  ## @param obs.enabled Enable/disable observability agent
  ##
  enabled: true
  ## @param obs.image image parameters
  ##
  image:
    ## @param obs.image.repository observability agent image name
    ##
    repository: ""
    ## @param obs.image.tag observability agent image tag
    ##
    tag: ""
    ## @param obs.image.pullPolicy observability agent image pull policy.
Defaults to 'Always' if image tag is 'latest', else set to 'IfNotPresent'
    ##
    pullPolicy: IfNotPresent
  ## @param obs.podAnnotations [object] Annotations to add to the pod for
observability (used for prometheus scraping)

```

```

##
podAnnotations: {}
## @param obs.podLabelsTemplate [object] Labels to add to the pod for
observability (used for pod monitoring) - can contain variables
##
podLabelsTemplate: {}
## @param obs.logs log management settings
##
logs:
  ## @param obs.logs.telemetry log telemetry config
  telemetry:
    ## @param obs.logs.telemetry.topic telemetry logs will be sent to this
Kafka topic
    topic: rbbn-otel-agent
  ## @param obs.logs.backendServers log backends
  ##
  backendServers: {}
    ## @param obs.logs.backendServers.elasticsearch elasticsearch backend
    ## Warning: username and password represent the name of the ENV variable
name
    ## that contains the username and password from the secret
    # elasticsearch:
    #   - endpoint: <elasticsearch server address>:443
    #     auth: True
    #     username: ELASTICSEARCH_USER
    #     password: ELASTICSEARCH_PASSWD
    #     index: <filebeat index>
    ## @param obs.logs.backendServers.kafka kafka backend
    ##
    # kafka:
    #   - endpoint: <kafka server address>:<kafka port>
    #     sslCert: KAFKA_CERT
    #     sslKey: KAFKA_KEY
    #     sslCa: KAFKA_CA
    ## @param obs.logs.elasticsearchSecretName Name of secret containing
elasticsearch environment variables
    ##
    elasticsearchSecretName: ""
    ## @param obs.logs.kafkaSecretName Name of secret containing elasticsearch
environment variables
    ##
    kafkaSecretName: ""

    ## @param obs.log.elasticsearchCreds elasticsearch credentials to create
    ##
    elasticsearchCreds:
      create: False
    ## @param obs.log.kafkaCreds kafka credentials to create
    ##
    kafkaCreds:
      create: False

```



```

## @section Common util
##
common-util:
  ## @param common-util.role Role for getting pod logs
  ##
  role:
    ## @param common-util.role.create Specifies whether a Role and RoleBinding
    should be created for the observability components
    create: false
  ## @param global.obs.serviceAccount SA for observability
  ##
  serviceAccount:
    ## @param common-util.serviceAccount.create Specifies whether a service
    account should be created for the observability components
    ##
    create: false
    ## @param common-util.serviceAccount.annotations Annotations to add to the
    service account
    ##
    annotations: {}
    ## @param common-util.serviceAccount.name The name of the service account
    to use.
    ## If not set and create is true, a name is generated using the fullname
    template
    ##
    name: default
  ## @param common-util.logPersistentVolumeStorage Storage request limit for
  PVC
  ##
  logPersistentVolumeStorage:
    ## @param common-util.logPersistentVolumeStorage.create Specifies whether
    to create a PVC for the storage of log entries
    ##
    create: true
    ## @param common-util.logPersistentVolumeStorage.storageClassName Specify
    the storageClass to be used for the PVC.
    ##
    storageClassName: "managed-nfs-storage"
  persistence:
    ## @param common-util.persistence.annotations Annotations to add to the
    PersistentVolumeClaims
    ##
    annotations:
      volume.beta.kubernetes.io/storage-provisioner: storage.io/nfs
  ## @param common-util.imageCredentials ImagePullSecret creation from
  credentials
  ##
  imageCredentials:
    ## @param common-util.imageCredentials.create Specifies whether an image
    credentials secret should be created
    ##
    create: true

```

```

    ## @param common-util.imageCredentials.createPostDelete Specifies whether
    an image credentials secret should be created as a post-delete hook
    ##
    createPostDelete: true
    ## @param common-util.prometheusRule Prometheus alerting rules
    ##
    prometheusRule:
      ## @param common-util.prometheusRule.create Specifies whether a
      PrometheusRule resource should be created
      ##
      create: false

```

Note

Repeat this procedure to set up all the three etcd instances on CNF. If you want to set up the third etcd instance on a VMware or KVM environment, refer to [RAMP CNF - Set up an etcd Cluster on Private Cloud](#).

View Etcd Member List

You can check the status of cluster synchronization and health of any node.

Prerequisites

The etcd cluster is up and running.

CNF etcd Status

To check the Etcd member list:

```

No certificates :
    etcdctl member list --write-out=table
certificates are enabled :
    etcdctl member list --cert=/opt/etcd/certs/client/cert.pem --key=/opt/etcd/
certs/client/key.pem --cacert=/opt/etcd/certs/client/ca.pem --write-out=table

```

Example output:

```

+-----+-----+-----+-----+
+-----+-----+-----+-----+
|      ID      | STATUS |      NAME      |      PEER ADDRS      |
| CLIENT ADDRS |        | IS LEARNER |      |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| 146c64bf5247d896 | started | sanetcdvmlr1-0 | https://10.52.61.153:2380 |
| https://10.52.61.153:2379 |      false |

```

```
| 3d5fea2b97cc6fa6 | started |          sanetcd | https://10.54.13.139:2380 | https://  
10.54.13.139:2379,https://127.0.0.1:2379 |      false |  
| b0555f0de8f1e2c1 | started |    sanetcdvm1-0 | https://10.52.144.154:2380 |  
https://10.52.144.154:2379 |      false |  
+-----+-----+-----+-----+  
+-----+-----+-----+-----+
```

etcd Health Status

To check the etcd health status:

```
$ etcdctl --endpoints=https://10.52.61.153:2379,https://10.54.13.139:2379,https://  
10.52.144.154:2379  
endpoint health --cert=/opt/etcd/certs/client/cert.pem --key=/opt/etcd/certs/client/  
key.pem --cacert=/opt/etcd/certs/client/ca.pem --write-out=table
```

Example output:

ENDPOINT	HEALTH	TOOK	ERROR
https://10.52.61.153:2379	true	9.535567ms	
https://10.54.13.139:2379	true	9.910137ms	
https://10.52.144.154:2379	true	1.069446076s	

Deploying RAMP with existing secret

In this section:

- [Generate RAMP certificates](#)
 - [Client Certificate](#)
 - [Create Secret for RAMP](#)

Generate RAMP certificates

Ribbon recommends using the TLS for communication between RAMP and ETCD. These certificates can be generated using the cert-manager, an extensible X.509 certificate controller for Kubernetes, or by using existing secrets. If the cert- manager is unavailable, the self-signed certificates can be used for RAMP to ETCD communication. The same Certificate Authority (CA) is used to generate self-signed certificates for both ETCD and RAMP. The following procedure explains how to generate self-signed certificates for RAMP-ETCD communication using the CFSSL tool.

Prerequisites

- The CA certificate is available. For more information, refer to [Generate Certificate Authority](#).

Create separate folders for each RAMP:

```
mkdir ~/certs/sanramp1
```

Client Certificate

1. Use **ramp** as Common Name.
2. The address filed should have SanS DNS and IP of RAMP.
3. The ca-config.json , ca.pem , ca-key.pem files are generated while creating CA.

```
mkdir ~/certs/sanramp1/client
cd ~/certs/sanramp1/client
export NAME=ramp
export ADDRESS=10.52.154.170,sanramp1-0-0.sanramp1-headless.ramp-
svt.svc.cluster.local,sanramp1-0-0,localhost,127.0.0.1,::1
echo '{"CN":"$NAME","hosts":[""],"key":{"algo":"rsa","size":2048}}' | cfssl
gencert -config=../../ca-config.json -ca=../../ca.pem -ca-key=../../ca-key.pem
-hostname="$ADDRESS" - | cfssljson -bare $NAME
```

4. Verify that the path for ca-config.json , ca.pem and ca-key.pem is correct.

```
# ls -ltr
total 12
-rw-r--r-- 1 root root 1460 May  8 17:07 ramp.pem
-rw-r--r-- 1 root root  924 May  8 17:07 ramp.csr
-rw----- 1 root root 1679 May  8 17:07 ramp-key.pem
```

5. Rename the files once the certificates are generated.

```
mv ramp.pem cert.pem
mv ramp-key.pem key.pem
```

Example output

```
# ls -ltr
total 12
-rw-r--r-- 1 root root  924 May  8 17:07 ramp.csr
-rw----- 1 root root 1679 May  8 17:07 key.pem
-rw-r--r-- 1 root root 1460 May  8 17:07 cert.pem
```

YAML File

```

global:

  # Namespace this helm chart will be deployed
  # This is optional. You could set to "" to use default namespace
  namespace: "ramp-svt"

  # Override obs storageClassName
  # This is optional. You could set to "" to use default storageClassName
  storageClassName: "managed-nfs-storage"

  ns_uuid: "nsuuid"
  cnf_uuid: "cnfuuid"
  cnfc_uuid: "cnfc_uuid"

  certManager:
    enabled: true
    issuer:
      name: "cross-cluster-ca-selfsigned-clusterissuer"
      ## @param global.certManager.issuer.kind The Issuer kind to sign the
      certificate request. Can be "Issuer" or "ClusterIssuer"
      kind: "ClusterIssuer"

  # This is used only for robin platform
  #pvcAnnotations:
  #  robin.io/faultdomain: host
  #  robin.io/media: SSD
  #  robin.io/replication: 3
  pvcAnnotations: {}

  auth:
    kafkaClient:
      secureTransport: false
      certFilename: cert.pem
      certKeyFilename: key.pem
      caFilename: "ca.pem"

      ## @param auth.client.certDuration Requested duration the signed certificate
      will be valid for
      certDuration: ""

      ## @param auth.client.certExtraDnsSans DNS Subject Alternative Name to add
      to the certificates
      certExtraDnsSans: ""

      ## @param auth.client.certExtraIpSans IP Subject Alternative Name to add to
      the certificates
      certExtraIpSans: ""

```

```

    ## @param auth.client.existingSecret Name of the existing secret containing
the TLS certificates for client-to-server communications
    existingSecret: ""
    # Base RBBN_OBS container image.
    # RCO: artifactory-tx.rbbn.com
    # BLR: artifact2.eng.sonusnet.com
    imageRegistry: artifact2.eng.sonusnet.com

# Values for init-container
# init container only installed when auth tls certs with existing Secret is used
rampinit:
    repository: ems-docker-prod-plano/production/rampcnf/rbbn-ramp-cnf-init
    pullPolicy: IfNotPresent
    tag: "24.03.00-450"

# If you need kubernetes secret to pull from private repo. You will need
username and access token
# For example:
# To get the access token:
# curl -u <windowsUsername>:'<windowsPasswd>' -X POST https://
artifact2.eng.sonusnet.com/artifactory/api/security/token -d
"username=<windowsUsername>" -d "expires_in=86400" -d "refreshable=true" -d
"scope=member-of-groups:readers" -d "audience=jfirt@"
# Replace windowUsername and windowPassword with appropriate username and
password.
# set imageCredentials: {} if you don't secret to pull from private repo
imageCredentials:
    create: false
    #Private repo for ribbon images
    registry: artifact2.eng.sonusnet.com
    username: ssequeira
    password:
eyJ2ZXIiOiIyIiwidHlwIjoiaSldUIiwiaWxnbWVudCI6ImYNTYiLCJraWQiOiJ0b2Z0emxGZGtnSjdaWFZnRn
RTTm94RzBLMTE3ZEZldEVaVXdsYVg3a2xVIn0.eyJzdWIiOiJqZnJ0QDAXY2RyYnJwejljYzclMXFnemI5
bTlxaHB1XC9lc2Vyc1wvc3NlcXVlaXJhIiwic2NwIjoibWVtYmVyLW9mLWdyb3Vwc3pyZWZkZXJzIiwiaXNz
VkIjoiamZydEAAQIiwiaXNzIjoiamZydEAAWmWNkcWJycHo5Y2M3NTFxZ3piOW0yMWhwZVwvdXNlcnNcL3Nz
ZXFlZWlyYSIsImV4cCI6MTcxOTcwNTc2NSwiaWF0IjoxNjg3NTY5NzY1LCJqdGkiOiIxMzQxMDhhNi02Nz
BmLTRhODktOTk1Mi04ODJjNGM5YmFkZDkifQ.W_0hudCJgQMF-
sIeA3NnOC85oNEKR90hyQW2mQcy4lgcJ4zihIrZHTwX5k43APCzPgW-
JpecRCh8jRJ9QmZzp56_7qSZXHc6VSWG5lc90ngWjhGCxq1lapQ75H1iFGmq8xP3e6GsebQMPGQqiloNK
4yEndKSXX9MRZcZ8Xu0z5Rczkf_MS00ppgxDtQmuEIWLyPJYsFPHYCYGcEfW_0LpkjptFHL-Io-
PHkW7SF-uIekubeAlKspPylHrh10QhghSntHm801cD_opc1V-
aV2J6L817vhaiaHUjxq5luZz_DTtA0vaFUFwmlsoTMTSH47Rff7VnMIe8kG0PY_dljig
    #If Customized Resource Name is needed, use the below section to populate the
details.
    #Currently customized resource name is applied only for configMap and Service
    #Make sure that the length of the customized resource is not exceeding 63
characters
    #If the servicePrefixTemplate/configmapPrefixTemplate are empty, then the
configmap and service will take the Release Name as the prefix
    customizedResourcePrefix:
    servicePrefixTemplate:

```

```

    ##servicePrefixTemplate: "svc-
    {{.Values.global.customizedResourcePrefix.robin.vendor_code}}-
    {{.Values.global.customizedResourcePrefix.robin.product_code}}-
    {{.Values.global.customizedResourcePrefix.robin.function_name}}"
    configmapPrefixTemplate:
    ##configmapPrefixTemplate: "cm-
    {{.Values.global.customizedResourcePrefix.robin.vendor_code}}-
    {{.Values.global.customizedResourcePrefix.robin.product_code}}-
    {{.Values.global.customizedResourcePrefix.robin.function_name}}"
    robin:
      vendor_code: rbbn
      product_code: ramp
      function_name: mno

# Override obs image for aggregator and agent
# This is required if you enable rbbn_obs (See below rbbn_obs.enabled = true)
obs:
  image:
    repository: ccs-docker-prod-virtual/rbbn_telemetry_collector
    tag: 3.1.0
    pullPolicy: Always

# Log rotation mechanism for the Observability server
obsLogRetentionPolicy:
# represent the percentage of the disk usage on when log rotation will be
trigger.
# I.e. A 20Gb storage limit request for a PVC with a rotateTriggerPercent set
at 50 (50%)
# means that log rotation will be trigger when disk will reach 10Gb
rotateTriggerPercent: 50
# Choice are "minute" "hourly" "daily" "weekly"
# recurringInterval represent the period of time on when we want to check if
disk usage has surpass the threshold.
recurringInterval: "hourly"

role:
# Specifies whether a Role and RoleBinding should be created for the
observability components
create: true

serviceAccount:
# Specifies whether a service account should be created for the
observability components
create: false
# Annotations to add to the service account
annotations: {}
# The name of the service account to use.
# If not set and create is true, a name is generated using the fullname
template
name: default

# Storage request limit for PVC

```

```

logPersistentVolumeStorage:
  use: false
  request: 20Gi
  annotations:
    volume.beta.kubernetes.io/storage-provisioner: storage.io/nfs

logs:
  # Name of secret that contains Elasticsearch credentials
  elasticsearchSecretName: ""
  # Name of secret that contains Elasticsearch credentials, evaluated as a
  template, for example "{{.Release.Name }}-elasticsearch-user-cred"
  elasticsearchSecretNameTemplate: ""
  # Name of secret that contains Kafka credentials
  kafkaSecretName: ""
  # Name of secret that contains Kafka credentials, evaluated as a template,
  for example "{{.Release.Name }}-kafka-user-cred"
  kafkaSecretNameTemplate: ""

  # Backend server configuration can be read here as an alternative to the
  obs.logs section
  backendServers:

common-util:
  # enabled: switch to enable or disable obs-common-modules
  # NOTE: Only one subchart per release can have this enabled.
  enabled: true
  prometheusRule:
    # Specifies whether a PrometheusRule resource should be created
    create: false
  role:
    # create: specify whether a Role and RoleBinding should be created for
    observability components
    # NOTE: If this is set to false, then the service account configured in
    global.serviceAccount.name
    # must have the following rules:
    # - apiGroups: [""]
    #   resources: ["pods"]
    #   verbs: ["get"]
    # - apiGroups: [""]
    #   resources: ["pods/log"]
    #   verbs: ["get"]
    # - apiGroups: ["metrics.k8s.io"]
    #   resources: ["pods"]
    #   verbs: ["get"]
    create: true
  imageCredentials:
    create: true
  logPersistentVolumeStorage:
    # create: specify whether a PVC should be created for observability
    create: true
    # storageClassName: name of the persistent storage class
    #storageClassName: netapp-nfs-san
  persistence:

```



```

    # persistence.annotations Annotations to add to the PersistentVolumeClaims
    annotations:
      volume.beta.kubernetes.io/storage-provisioner: storage.io/nfs
    imageCredentials:
      # Specifies whether an image credentials secret should be created as a post-
delete hook
      createPostDelete: true
    prometheusRule:
      # Specifies whether a PrometheusRule resource should be created
      create: false

#Timezone for ramp pod
# This is optional. Comment it out if not needed. It will default to UTC if not
provided.
timeZone: "Asia/Kolkata"

# Platform on which the Ribbon RAMP CNE solution is deployed.
# Allowed values - ocp, robin
kubernetesPlatform: ocp

# robin platform wants to be able to specify static_ip_policy in annotations
# accepted values are ippool,range
static_ip_policy: "ippool"

# Template strings to evaluate to existing secret to use to pull images, for
example: name: "{{.Release.Name }}-imagecred"
imagePullSecretTemplates:
  - name: "{{.Release.Name }}-imagecred"

# Values for rbbn-ramp chart
rbbn-ramp:
  #Ramp image
  # This is required
  rampImage:
    repository: ems-docker-prod-plano/production/rampcnf/rbbn-ramp-cnf
    pullPolicy: IfNotPresent
    # This is the ramp version
    tag: "24.03.00-450"
    #tag: "22.05.00-131"

# Define addition external interfaces for ramp pod
# This is required. Ramp requires eth1 for management access.
networkInterface:
  # Either 'ipv4' or 'ipv6'
  ipversion: "ipv4"
  #Number of external interface for ramp
  numberOfExternalInterface: 1
  # This is the interface for management access - devices, GR, etc.
  eth1:
    interface: ext-whereabouts-net-1
    ip: "10.52.154.170"
    prefix: "24"
    gateway: "10.52.154.1"

```

```

routes:
  - destIp: "10.70.0.0"
    prefix: "16"
  - destIp: "10.54.0.0"
    prefix: "16"
  - destIp: "172.19.0.0"
    prefix: "16"
  - destIp: "172.21.0.0"
    prefix: "16"
  - destIp: "172.23.0.0"
    prefix: "16"
  - destIp: "172.29.0.0"
    prefix: "16"
  - destIp: "172.28.0.0"
    prefix: "16"
  - destIp: "172.16.0.0"
    prefix: "16"
  - destIp: "10.228.0.0"
    prefix: "16"

# Ramp kubernetes service
# "port" exposes the Kubernetes service on the specified port within the
cluster. Other pods within the cluster can communicate with this server on the
specified port
# "type" could be "ClusterIP", "NodePort" and "LoadBalancer". Refer to
kubernetes service for more detail.
# Set enabled: false if not needed.
rampService:
  enabled: false
  port: 443
  type: ClusterIP

auth:
  # etcd client TLS certificate
  enabled: true
  etcdclient:
    certManager:
      # enabled: switch to enable cert-manager to generate and manage the etcd
client certificate
      # NOTE: Set this to true only if global.certManager.enabled is set to true
and network.interfaceName
      # is set to eth1 and the network attachment used for eth1 is configured to
assign static IPs.
      enabled: true
      ## @param auth.client.certExtraDnsSans DNS Subject Alternative Name to add
to the certificates
      ##
      certExtraDnsSans: ""
      ## @param auth.client.certExtraIpSans IP Subject Alternative Name to add
to the certificates
      ##
      certExtraIpSans: ""

```

```

    # certDuration: duration in hours, minutes, or seconds that the
certificate should be valid for
    # NOTE: If certDuration is not specified (""), then the certificate will
be valid
    # for 90 days by default and will be renewed 30 days before expiry. The
minimum value for
    # certDuration is 1 hour.
    # Example:
    # If the duration needs to be 180 days, then this can be specified as
below:
    #   certDuration: 4320h
    certDuration: ""
    ## auth enabled is true and cerManager enabled is false then existing
secret is used
    existingSecret: ""

alarm:
  exporters:
    - enabled: true
    type: kafka
    config:
      bootstrap_servers:
        - ip: 172.19.57.140
        port: 9092
      topic: "ramp-svt"
      format: json
      standard: ETSI_S0L003
      properties: # producer configuration can be provided here with proper
indentation
    #   security.protocol: SSL
    #   ssl.kafka.private.key.location: /opt/fm/kafka/certs/key.pem
    #   ssl.kafka.public.cert.location: /opt/fm/kafka/certs/cert.pem
    #   ssl.kafka.ca.cert.location: /opt/fm/kafka/certs/ca.pem

    # The memory/cpu limits will be equals to requests to ensure pod gets assigned a
QoS class of Guaranteed
    # Required
    rampResources:
      requests:
        cpu: 16
        memory: 64Gi
    #   hugepages:
    limits:
    #   hugepages: 2Gi

    # Persistent for ramp container
    rampPersistent:
      #Storage class class for ramp. User could configure different
storageClassName for obs(global section)
      #storageClass is optional field.
      #storageClassName is optional. Comment it out if you want to use default
storageClassName.
      storageClassName: "csi-rbd-sc"

```

```

# storageAccessMode for ramp
#ReadWriteOnce - the volume can be mounted as read-write by a single node
#ReadOnlyMany - the volume can be mounted read-only by many nodes
#ReadWriteMany - the volume can be mounted as read-write by many nodes
# storageAccessMode is required field
storageAccessMode: "ReadWriteOnce"

# Storage size. Required field.
storage: "130Gi"

# Enable or disable startupProbe, livenessProbe, and readinessProbe
probe: True

#Assigning Pods to Nodes with specific label
#For example:
nodeSelector: {}
#nodeSelector:
# kubernetes.io/hostname: worker-9.blr-ocp1.lab.rbbn.com

# Set this for kubernetes tolerations
# Optional
tolerations: []

# Set this for kubernetes affinity
# Optional
affinity: {}

# Set the namespaces for antiaffinity rule
anti_affinity_namespaces: ["sbc-svt-regr", "psx-svt", "ems-dev", "ems-svt-perf",
"ems-svt", "ats-dev", "ems-svt-2", "platform-dev", "platform-svt", "psx-dev", "raf-dev",
"rampev-svt", "sbx-dev", "sbc-svt", "psx-cnf-svt", "cnf-demolab", "sbc-dev-tekton",
"ramp-svt", "ems-svt-perf", "cats-svt", "rbbn-ses-na"]

#Use this to inject public keys for users. Set it to
# Optional
#Users: [] if not needed.
users:
- name: "admin"
  # To generate password for "admin" user, run "openssl passwd -6 admin"
  password: "$6$1QMeZQPJoaXfchXn$2jYBgDqj9ubRTRMgPwoDQg87358IBY7pV9FmBf/
VNN57htbOWP9DezDgXp30mo7LthuHbDjFekrAWxB8UQ/tt1"
  ssh_authorized_keys:
    - ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIE1q9aASBnezCE+irhepjZrZSuY4w0hkNBUyQ0uqnCgeT admin@rbbn.co
m
- name: "insight"
  # To generate password for "insight" user, run "openssl passwd -6 insight"
  password: "$6$WDZgaeEQY007xZLg$SVZ/OQL/.VUF/dFu/
1M.rxfNq0JdxSXNHCiPqKwduuyoS0y6iLnN2kZ/qbLhMVVDwarQYmbCB22C9pGZ.BT8f1"
  ssh_authorized_keys:

```

```

- ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIE1q9aASBnezCE+irhepjrzSuY4wOhkNBUyQ0uqnCgeT insight@rbbn.
com

# You only need to modify this if you want to use rbbn-sdrp
# Set enabled: true if you want to enable sdrp for ramp. Default to false
rbbn_sdrp:
  enabled: false
  common_name: ""
  fqdn_domain: ""

# You only need to modify this if you want to use rbbn-obs
# Set enabled: true if you want to enable observability agent for ramp. Default
to true
rbbn_obs:
  enabled: true

# Service for obs sidecar within pod.
obsService:
  type: ClusterIP
  port: 9101
  ipFamilyPolicy: SingleStack # Allowed values PreferDualStack or
SingleStack.According the below value should be altered
  ipFamilies:
    - IPv4

resources:
  rbbn_telemetry_agent:
    limits:
      cpu: 4
      memory: 8Gi
    #requests:
    #  cpu: 100m
    #  memory: 128Mi

# Add the pod annotations to enable prometheus discovery and scraping.
# port we are exposing for prometheus scraping.
# This port should match the service port and the server metric output
endpoint.
podAnnotations:
  prometheus.io/path: "/metrics"
  prometheus.io/scrape: true
  prometheus.io/port: "9101"
  prometheus.io/scheme: "http"

serviceLabels:
  component: prometheus-rbbn-otel-agent
  tenant: ramp
  servicetype: observability

configMap:
  metrics:

```

```

    enable: True
    appStats:
      scrapeInterval: 5s
      endpoints:
        - addr: "localhost:10050"
          containerName: rbbn-rampcnf-container
    output:
      - server: "prometheus"
        endpoint: "0.0.0.0:9101"
  logs:
    enable: True
    defaultTopic: rampsvtdefault # log messages to this Kafka topic by default
when a topic for the container parsers or system is not specified
    telemetry:
      enable: True # Process the otel agent logs
      topic: ramprrbn-otel-agent # Open telemetry logs will be sent to this
Kafka topic
    podlogs: True
    logPrefix:
      nodeId: True
      containerId: True
    backendServers: # Example of backend servers
      stdout:
        enable: False
      elasticsearch: []
        # - endpoint: elasticsearch.apps.rco-ocp1.lab.rbbn.com:443
        #   auth: True
        #   username: ELASTICSEARCH_USER
        #   password: ELASTICSEARCH_PASSWD
        #   index: platform-filebeat
      kafka:
        - endpoint: 172.19.57.140:9092
          PROTOCOL: PLAINTEXT
        # - endpoint: elasticsearch.apps.rco-ocp1.lab.rbbn.com:12345
        #   sslCert: KAFKA_CERT
        #   sslKey: KAFKA_KEY
        #   sslCa: KAFKA_CA
# elasticsearch Credentials
elasticsearchCreds:
  create: False
  #user:
    #key: ELASTICSEARCH_USER
    #value:
  #password:
    #key: ELASTICSEARCH_PASSWD
    #value:
# KAFKA Credentials
# all values should be base64 encoded.
kafkaCreds:
  create: False
  path: /etc/kafka/ssl
  sslCert:
    key: KAFKA_CERT

```

```

        value:
      sslKey:
        key: KAFKA_KEY
        value:
      sslCa:
        key: KAFKA_CA
        value:

## sdrp subchart values
sdrp-operator:
  ## @section roles parameters
  roles:
    create: true
  ## @section Prometheus Rule
  prometheusRule:
    ## @param prometheusRule.create Specifies whether a PrometheusRule resource
    should be created (alerting rule definitions)
    create: false
  common-util:
    # required for sdrp-operator obs Agent
    logPersistentVolumeStorage:
      create: false
    imageCredentials:
      # Specifies whether an image credentials secret should be created as a post-
      delete hook
      createPostDelete: true
    ## @param common-util.prometheusRule Prometheus alerting rules
    prometheusRule:
      ## @param common-util.prometheusRule.create Specifies whether a
      PrometheusRule resource should be created
      create: false
  ## @section sdrp-operator container parameters
  operator:

    ## @param sdrp-operator image parameters
    image:
      ## @param operator.image.repository sdrp-operator image name
      repository: ccs-docker-prod-virtual/sdrp-operator

  ## @section sdr container parameters
  ##
  ## @param sdr.clusterScopeRegistry.enabled Create a backend configuration for
  the cluster scope if equal true
  ## @param sdr.globalScopeRegistry Specify the initial backend configuration for
  the global scope to use in the sdr container
  ## @param nameservers - [array] List of DNS nameserver. Syntax: ip:port. If
  port if not specified, port 53 is used
  ## @param domain - Name of the domain to publish to in the service registry for
  the cluster scope
  ## @param tsigKeyName - Name of the TSIG key attached to DNS messages
  ## @param tsigSecret - TSIG (base64) value attached to DNS messages
  ## @param tsigSecretAlg - TSIG algorithm. Supported value: hmac-md5, hmac-sha1,
  hmac-sha256, hmac-sha512

```

```
##
sdr:
  ## @param sdrp-operator image parameters
  image:
    ## @param operator.image.repository sdrp-operator image name
    repository: service_discovery-docker-prod-ottawa/sdr

  clusterScopeRegistry:
    enabled: true
    nameservers: []
    domain: ""
    tsigKeyName: ""
    tsigSecret: ""
    tsigSecretAlg: ""
  globalScopeRegistry:
    enabled: true
    nameservers: []
    domain: ""
    tsigKeyName: ""
    tsigSecret: ""
    tsigSecretAlg: ""
```

Create Secret for RAMP

```
$ cd ~/certs/sanramp1/client
$ kubectl create secret generic sanramp1-certs --from-file=../../ca.pem --from-
file=key.pem --from-file=cert.pem
```

Example output:

```
$ kubectl create secret generic sanramp1-certs --from-file=./ca.pem --from-file=key.pem
--from-file=cert.pem
secret/sanramp1-certs created
$ oc get secret | grep sanramp1-certs
sanramp1-certs                Opaque                3                42s
```

Create a secret client for RAMP:

Enabling SSL for Kafka Forwarder

Ribbon recommends using TLS for communication between RAMP and the Kafka server. Certificates can be generated using cert-manager, an extensible X.509 certificate controller for Kubernetes, or by utilizing existing Secrets. If cert-manager is not available in Kubernetes, self-signed certificates can be used for RAMP to Kafka

server communication. The same CA should be used for generating self-signed certificates for both the Kafka server and RAMP. The following procedure outlines how to generate self-signed certificates for RAMP-Kafka communication using the CFSSL tool.

Prerequisites

- The CA certificate is available. For more information, refer [Generate Certificate Authority](#).

Kafka Forwarder Client Certificate

- Create a folder for Kafka Forwarder certificate:

```
mkdir ~/.certs/sanrampkafka
```

- To create client certificate for Kafka forwarder, perform the following:
 - Use **ramp** as Common Name.
 - The address filed should have SanS DNS and IP of RAMP.
 - The ca-config.json , ca.pem , ca-key.pem files are generated while creating CA.

```
mkdir ~/.certs/sanrampkafka/client
cd ~/.certs/sanrampkafka/client
export NAME=ramp
export ADDRESS=10.52.154.170,sanramp1-0-0.sanramp1-headless.ramp-
svt.svc.cluster.local,sanramp1-0-0,localhost,127.0.0.1,::1
echo '{"CN":"'$NAME'", "hosts":[""], "key":{"algo":"rsa", "size":2048}}' | cfssl
gencert -config=../../ca-config.json -ca=../../ca.pem -ca-key=../../ca-key.pem
-hostname="$ADDRESS" - | cfssljson -bare $NAME
```

- Verify that the path for ca-config.json , ca.pem and ca-key.pem is correct.

```
# ls -ltr
total 12
-rw-r--r-- 1 root root 1460 May  8 17:07 ramp.pem
-rw-r--r-- 1 root root  924 May  8 17:07 ramp.csr
-rw----- 1 root root 1679 May  8 17:07 ramp-key.pem
```

- Rename the files once the certificates are generated.

```
mv ramp.pem cert.pem
mv ramp-key.pem key.pem
```

Example Output:

```
# ls -ltr
total 12
-rw-r--r-- 1 root root  924 May  8 17:07 ramp.csr
```

```
-rw----- 1 root root 1679 May  8 17:07 key.pem
-rw-r--r-- 1 root root 1460 May  8 17:07 cert.pem
```

Create Secret for Kafka Forwarder

Create a secret client for Kafka Forwarder:

```
$ cd ~/certs/sanrampkafka/client
$ kubectl create secret generic sanramp1-kafka-certs --from-file=../ca.pem --from-
file=key.pem --from-file=cert.pem
```

Example Output:

```
$ kubectl create secret generic sanramp1-kafka-certs --from-file=../ca.pem --from-
file=key.pem --from-file=cert.pem
secret/sanramp1-kafka-certs created
$ oc get secret | grep sanramp1-kafka-certs
sanramp1-kafka-certs          Opaque          3
42s
```

To enable SSL for Kafka Forwarder, the following changes are required in the RAMP values.yaml:

```
auth:
  kafkaClient:
    secureTransport: true
    certFilename: cert.pem
    certKeyFilename: key.pem
    caFilename: "ca.pem"

    ## @param auth.client.certDuration Requested duration the signed certificate will be
    valid for
    certDuration: ""

    ## @param auth.client.certExtraDnsSans DNS Subject Alternative Name to add to the
    certificates
    certExtraDnsSans: ""

    ## @param auth.client.certExtraIpSans IP Subject Alternative Name to add to the
    certificates
    certExtraIpSans: ""

    ## @param auth.client.existingSecret Name of the existing secret containing the TLS
    certificates for client-to-server communications
    existingSecret: "sanramp1-kafka-certs"

alarm:
  exporters:
    - enabled: true
```

```

type: kafka
config:
  bootstrap_servers:
    - ip: 172.19.57.140
      port: 9093
    - ip: 172.19.57.141
      port: 9093
  topic: "ramp-svt"
  format: json
  standard: ETSI_S0L003
  properties: # producer configuration can be provided here with proper
indentation
    security.protocol: SSL
    ssl.kafka.private.key.location: /opt/fm/kafka/certs/key.pem
    ssl.kafka.public.cert.location: /opt/fm/kafka/certs/cert.pem
    ssl.kafka.ca.cert.location: /opt/fm/kafka/certs/ca.pem

```

Deploying etcd with Existing Secret

In this section:

- [Generate etcd certificates](#)
 - [Client Certificate](#)
 - [Peer Certificate](#)
 - [Create a Secret for ETCD](#)

Generate etcd certificates

Ribbon recommends using TLS to communicate between the Ribbon Application Management Platform (RAMP) and etcd and between the etcd nodes. You can generate certificates using the cert-manager, an extensible X.509 certificate controller for Kubernetes, or using existing secrets. If the cert-manager is unavailable, you can use self-signed certificates for both RAMP-to-etcd and etcd-to-etcd communications. Use the same Certificate Authority (CA) to generate self-signed certificates for etcd and RAMP. Ribbon recommends creating and signing a new key pair for each member in a cluster.

The following procedure outlines how to generate self-signed certificates for RAMP to etcd and etcd to etcd communication using the CFSSL tool:

Note

Generate and sign a new key pair for each member in a cluster. The etcd instances require two sets of TLS certificates: one for serving client requests and another for the peer endpoint for inter-member communication.

Prerequisites

- The CA certificate is available. For more information, refer to [Generate Certificate Authority](#).

The following procedure explains how to create self-signed certificates for both client and peer communication:

Create separate folders for each etcd:

```
mkdir ~/certs/etcdtrial
```

Client Certificate

Use the following procedure to create a client certificate:

Start

1. Set the name of etcd as a common name.
2. The address filed should have SanS DNS and IP of etcd.
3. The files `ca-config.json` , `ca.pem` , `ca-key.pem` are generated when creating a Certificate Authority (CA).

```
mkdir ~/certs/etcdtrial/server-client
cd ~/certs/etcdtrial/server-client
export NAME=etcdtrial
export ADDRESS=172.21.224.124,etcdtrial-0-0.etcdtrial-headless.ramp-
svt.svc.cluster.local,etcdtrial-0-0,localhost,127.0.0.1,::1
echo '{"CN":"'${NAME}',"hosts":[""],"key":{"algo":"rsa","size":2048}}' | cfssl
gencert -config=../../ca-config.json -ca=../../ca.pem -ca-key=../../ca-key.pem
-hostname="$ADDRESS" - | cfssljson -bare $NAME
```

4. Verify whether the path for `ca-config.json` , `ca.pem` , and `ca-key.pem` is correct:

```
# ls -ltr

total 12

-rw-r--r-- 1 root root 1472 May  9 01:02 etcdtrial.pem
-rw-r--r-- 1 root root  932 May  9 01:02 etcdtrial.csr
-rw----- 1 root root 1675 May  9 01:02 etcdtrial-key.pem
```

5. Rename the files after generating the certificates:

```
# mv etcdtrial.pem cert.pem
# mv etcdtrial-key.pem key.pem
```

Peer Certificate

Perform the following to create a Peer Certificate:

Start

1. The Common Name for `etcd-peer` should be set as such, as it is hardcoded in the ETCD stateful set configuration.
2. The address files should have SanS DNS and ETCD IP.
3. The `ca-config.json` , `ca.pem` , `ca-key.pem` files are generated while creating CA.

```
mkdir ~/certs/etcdtrial/peer
cd ~/certs/etcdtrial/peer
export NAME=etcd-peer
export ADDRESS=172.21.224.124,etcdtrial-0-0.etcdtrial-headless.ramp-
svt.svc.cluster.local,etcdtrial-0-0,localhost,127.0.0.1,::1
echo '{"CN": "'$NAME'", "hosts": [""], "key": {"algo": "rsa", "size": 2048}}' | cfssl
gencert -config=../../ca-config.json -ca=../../ca.pem -ca-key=../../ca-key.pem
-hostname="$ADDRESS" - | cfssljson -bare $NAME
```

4. Verify whether the path for ca-config.json , ca.pem, and ca-key.pem is correct.

```
# ls -ltr
total 12
-rw-r--r-- 1 root root 1472 May  9 01:04 etcd-peer.pem
-rw-r--r-- 1 root root  932 May  9 01:04 etcd-peer.csr
-rw----- 1 root root 1679 May  9 01:04 etcd-peer-key.pem
```

5. Rename the files after generating the certificates.

```
# mv etcd-peer.pem cert.pem
# mv etcd-peer-key.pem key.pem
```

Example output:

```
# ls -ltr
total 12
-rw----- 1 root root 1679 May  9 01:04 key.pem
-rw-r--r-- 1 root root  932 May  9 01:04 etcd-peer.csr
-RW-r--r-- 1 root root 1472 May  9 01:04 cert.pem
```

Create a Secret for ETCD

Perform the following to create a Secret certificate for ETCD.

Start

1. Generate Secret for ETCD server-client certificates:

```
cd ~/certs/etcdtrial/server-client
kubectl create secret generic etcd-client-certs --from-file=../../ca.pem --from-
file=key.pem --from-file=cert.pem
```

Example output:

```
$ kubectl create secret generic etcd-client-certs --from-file=../../ca.pem --from-
file=key.pem --from-file=cert.pem
secret/etcd-client-certs created
$ oc get secret | grep etcd-client-certs
etcd-client-certs
Opaque                                3          14s
```

2. Generate Secret peer for ETCD:

```
cd ~/certs/etcdtrial/peer
kubectl create secret generic etcd-peer-certs --from-file=../../ca.pem --from-
file=key.pem --from-file=cert.pem
```

Example output

```
$ cd ~/certs/etcdtrial/peer
$ kubectl create secret generic etcd-peer-certs --from-file=../../ca.pem --from-
file=key.pem --from-file=cert.pem
secret/etcd-peer-certs created

$ oc get secret | grep etcd-peer-certs
etcd-peer-certs
Opaque                                3          32s
```

3. Repeat the same steps for all ETCDs.

Note

Two sets of ETCD certificates are required if the both Client/Server uses the same peer certificates. The same two sets can also be used for other two ETCDs.

RAMP CNF - Set up an etcd Cluster on Private Cloud

In this section:

- [Set up etcd VMs on VMware](#)
 - [Create an ISO Configuration Drive for VMware](#)
 - [Create the etcd VMs Using the VMware GUI](#)
 - [Customize VMware Settings](#)
- [Set up the etcd VMs on KVM](#)

Related articles:

- [Configuring RAMP GR with Automatic Switchover Enabled](#)
- [Deployment Models](#)
- [RAMP Security Group Rules](#)
- [Configuring RAMP Redundancy](#)
- [Managing Redundancy](#)

- Create an ISO Configuration Drive for KVM
- Create the etcd VMs on a KVM Platform
- Set up etcd VMs on OpenStack
- Health Check etcd
 - Prerequisites
 - Health check on etcd
- Renew Certificates on VMware and KVM etcd

For the purposes of monitoring a RAMP Geographically Redundant (GR) deployment to enable automatic switchover, three etcd VMs are required. Refer to [Configuring RAMP GR with Automatic Switchover Enabled](#) for information on how the etcd VMs are involved in the GR deployment. You can instantiate these VMs on VMware, KVM, or OpenStack. VMs instantiated on VMware and KVM connect to CNF etcd for AppServices with version 23.03 and above. You are not required to deploy the etcd VMs on the same platform as the RAMP instances.

Prerequisites

- Three free IP addresses are available to allocate to the etcd instances.
- The recommended configuration is 1 vCPU and 2GB of memory. For more information, refer to [RAMP etcd System Requirements](#).

Set up etcd VMs on VMware

To set up etcd on VMware-based VMs, first create an ISO configuration drive.

Create an ISO Configuration Drive for VMware

Complete the following procedure to set up an ISO configuration drive.

Start

1. Log on to the Ribbon Support portal. Download the `AppServices-configDrive.img` and the `AppServices-xx.xx.xxRxxx-xxxxx_vmCCS-x.x.x-xxxxx-xxx_xx.vmdk` files (refer to the release notes for the .vmdk file name). For more information on using the portal, refer to [Downloading Files from Ribbon Support Portal](#).
2. Log on to a Linux server as the root user. On this server you will create an `.iso` file from the provided template file (`AppServices-configDrive.img`) to use as a configuration drive for the VMs.
3. Create a temporary directory. In the following example the directory name is "etcd."

```
mkdir -p /tmp/etcd
```

4. Mount the image.

```
sudo mount AppServices-configDrive.img /tmp/etcd
```

5. Edit the cloud configuration.

```
vim /tmp/etcd/user-data
```

[Click to view parameter details...](#)

Parameters To Edit	Description	Example	Notes
hostname	Hostname of the VM in use.	hostname: "ammanetcd"	
fqdn	FQDN of the VM in use.	fqdn: "ammanetcd.local.com"	
timezone	Choose the time zone.	timezone: "Asia/Kolkata"	
ntp	NTP server IP.	servers: ["10.128.254.67"]	
Users Info	Information on the users created.	users: - name: root plain_text_passwd: "root" lock_passwd: false - name: sysadm plain_text_passwd: "sysadm" lock_passwd: false - name: "backup_user" plain_text_passwd: "shipped!!" lock_passwd: false groups: backup_group	Provide details of the users that are created.

Parameters To Edit	Description	Example	Notes
content	Persistent hostname file	<pre>write_files: # Persistent hostname file - content: "ammanetcd" # Must match 'fqdn' value above</pre>	

Parameters To Edit	Description	Example	Notes
VnfName GatewayIpv4/ GatewayIpv6 ExternalIp	Name of the VNF as in "ammanetcd" Gateway IP address of the etcd instance IP address of the etcd instance	# Ribbon vmCCS userdata: - content: { "VnfName": "ammanetcd",	◦ Net{1,2,3}: Definition for the interface IF{1,2,3} ◦ Enabled : Indicates if the interface is enabled. Enabled is mandatory. It must be set to "true" or "false". ◦ GatewayIpv4: IPv4 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface ◦ GatewayIpv6: IPv6 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface ◦ ExternalIp: External IP address for this interface ◦ Categories: List of category of traffic on this interface. By default, management is on net1, signaling and internal are on net2, and nothing is configured for net3.

Parameters To Edit	Description	Example	Notes
		<pre> "Networks": { "Net1": { "Enabled": "True", "GatewayIpv4": "10.54.8.1", "GatewayIpv6": "", "Externallp": "10.54.8.166", "Categories": [], "IsDefault": "True" }, "Net2": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "Externallp": "", "Categories": [], "IsDefault": "" }, "Net3": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "Externallp": "", "Categories": [], "IsDefault": "" } }, </pre>	◦ IsDefault: Indicates whether the default route should be assigned to this interface. Only one interface may have IsDefault=true. If false for all interfaces, the first interface with a gateway configured will be assigned the default route. This parameter is not required if only one gateway was specified in the network-config file.

Parameters To Edit	Description	Example	Notes
UseEtcd	enable etcd	<pre># Ribbon AppServices userdata: fill in all fields according to user guide - content: { "UseEtcd" : "True", }</pre>	Enable the etcd ansible playbooks to be triggered after installation.
ExistingEndpoints NOTE: This parameter is specifically for connections from etcd vnf to etcd cnf . Do not provide "EtcdRegistries" and "VnfExistingInstances".	Add all the endpoints from CNF environment setup.	<pre>"Etcd": { "ExistingEndpoints" : ["https:// 10.52.61.154:2379" ,"https:// 10.52.61.155:2379"],</pre>	While creating the third instance, "ExistingInstances" must contain the ClientURL of the first and second etcd instances that were created.
Certificates NOTE: This parameter is specifically for connections from etcd vnf to etcd cnf. Do not provide "EtcdRegistries" and "VnfExistingInstances"	Certificate to enable mtls for communication	<pre>"ClientCert" : "ClientKey" : "ClientCaCert" : "ServerCert" : "ServerKey" : "ServerCaCert" : "PeerCert" : "PeerKey" : "PeerCaCert" :</pre>	Client Cert/key/ca: for etcdctl communication. Peer Certificates for communication between other etcds in cluster. Server Certificates for serving client requests on port "2379". The Certificates should have same root certificate as CNF Etcd Created. NOTE: Once the CertFiles are generated. replace line breaks with "\n" to add them to parameters. To create certificates, see https://cert-manager.io/docs/usage/certificate/

Parameters To Edit	Description	Example	Notes
Etcd	Etcd configuration	<pre> "Etcd": { "ExistingEndpoints" : [], "PersistentDataPath" : "", "PersistentBackupPath" : "", "RootPassword" : "", "UserName" : "", "UserPassword" : "", "ClientCert" : "", "ClientKey" : "", "ClientCaCert" : "", "ServerCert" : "", "ServerKey" : "", "ServerCaCert" : "", "PeerCert" : "", "PeerKey" : "", "PeerCaCert" : "", "HeartbeatInterval" : "", "ElectionTimeout" : "", "BackupDiskMaxUse" : "", "BackupDiskKeepFree" : "" </pre>	◦ PersistentDataPath: Path to the persistent disk to use for Etcd data. The virtio number corresponds to the Etcd data volume ID provided in the deployment. ◦ RootPassword: The Etcd database password for the root user. If left blank, no authentication is enabled on the database. In a HA setup, the passwords must match on all the virtual machines. ◦ UserName: The name of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank. ◦ UserPassword: The password of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank.

Parameters To Edit	Description	Example	Notes
		<pre>"BackupStartTime" : "", "BackupFullPeriod" : "0", "BackupRetention" : "" },</pre>	◦ HeartbeatInterval: The interval (in ms) at which the leader notifies followers that it is still the leader. The recommended value to set is around the maximum of average round-trip time (RTT) between members, it is normally around 0.5-1.5x the round-trip time. If this field is left blank or omitted, the default value is 100 ms. ◦ ElectionTimeout: The duration (in ms) that a follower node performs without hearing a heartbeat before attempting to become the leader. The recommended value to set must be at least 10 times the RTT to account for a variance in the network. If this field is left blank or omitted, the default value is 1000 ms. ◦ BackupDiskMaxUse: The maximum percentage of the disk that allowed to be occupied by the Etcd backup files. The default value is 15.

Parameters To Edit	Description	Example	Notes
			◦ BackupDiskKeepFree : The percentage of disk that must be left free on the file system. The oldest backup files are deleted when this limit is reached. The default value is 30. ◦ BackupStartTime : The time of day when the scheduled backup starts. The format is in hh:mm±hh:mm. The first part of the format is the start time and second part is an offset (from UTC) to specify the time zone. If the time zone is not specified, then the local time zone of the virtual machine processing the request is used as the default time zone. The default value is 02:00. ◦ BackupFullPeriod : The interval at which a full backup of the Etc full is performed. This is expressed in the format of weeks and/or days, or hours. For example, 1w2d or 4h. Hours are not allowed to be provided with days or weeks. • The maximum allowed value for hours is 23h.

Parameters To Edit	Description	Example	Notes
			- The minimum allowed value is 1h. 0 means that no backup is performed. The default value is 1d. NOTE: Set the <code>BackupFullPeriod</code> as 0 (Zero). <code>BackupRetention</code>: Specifies how long the backup files are retained before deleting the file(s). An empty value means that the backup files are retained for 7 days. This is expressed in the format of weeks, days and/or hours. For example, 1w24h or 2d.
EtcRegistries NOTE: Ignore this if you are instantiating a connection from vnf etcd to the CNF etcd.	IP addresses of any etcd instances created before	<pre>"VnfOperations": { "EtcRegistries": ["10.54.8.166", "10.54.8.165"], "EtcUserName": "admin", "EtcUserPassword": "admin", "Salt": "mysalt@123" }</pre>	While creating the first instance, "EtcRegistries" does not contain any value. While creating the second instance, "EtcRegistries" must contain the IP address of first etcd instance that was created. While creating the third instance, "EtcRegistries" must contain the IP addresses of the first and second etcd instances that were created. You can ignore this if you are setting a vnf etcd to connect to the CNF etcd.

Parameters To Edit	Description	Example	Notes
VnfExistingInstances NOTE: Ignore this if you are instantiating a connection from vnf etcd to connect to the CNF etcd.	IP addresses of any etcd instances created before	"VnfExistingInstances" : ["10.54.8.166","10.54.8.165"], "VnfReplaceInstance" : "", "UseMongoDB" : "", "UseEtcd" : "True", "UsePrometheus" : "", "UseAlertManager" : ""	While creating the first instance, "VnfExistingInstances" does not contain any value. While creating the second instance, "VnfExistingInstances" must contain the IP address of first etcd instance that was created. While creating the third instance, "VnfExistingInstances" must contain the IP addresses of the first and second etcd instances that were created.

6. Edit the network configuration:

```
vim /tmp/etcd/network-config
```

Edit the following parameters in the network-config file:

Parameters To Edit	Description	Example
addresses gateway4/gateway6	IP address to assign to this interface. The default gateway.	# DO NOT CHANGE version: 2 # List of network interfaces ethernets: # Network 1 eth0: addresses: # List of IP[v4,v6] addresses to assign to this interface - 10.54.48.60/23 # example: 10.20.30.5/24, fd00:10:6b50:5180::24/60 # Disable if not using IPv4 gateway4: "10.54.48.1" # Default IPv4 gateway, can be moved to another interface if desired (example: default gateway on eth2) # Enable if using IPv6 gateway6: "" # Default IPv6 gateway, can be moved to another interface if desired (example: default gateway on eth2)

7. Issue the `genisoimage` command to create the `.iso` file:

```
genisoimage -o etcd.iso -V cidata -r /tmp/etcd
```

8. After creating the `.iso` file, remove the temporary `etcd` directory:

```
sudo umount /tmp/etcd
rm -rf /tmp/etcd
```

The ISO configuration is now complete.

9. Copy the `.iso` file created and the `AppServices-xx.xx.xxRxxx-xxxxx_vmCCS-x.x.x-xxxxx-xxx_xx.vmdk` files (refer to the release notes for the `.vmdk` file name) to the VMware host datastore location (`/vmfs/volumes/datastore1/etcdvnf`).
10. Create copies of the VMDK files, one for each VM, and then convert the copies to thin format using the following command:

```
vmkfstools -i AppServices-22.07.00R000-B3500_vmCCS-1.4.1-B2297-
x86_64.vmdk AppServices-22.07.00R000-B3500_vmCCS-1.4.1-B2297-
x86_64_converted.vmdk -d thin
```

Create the etcd VMs Using the VMware GUI

Complete the following steps to instantiate the etcd VMs using the VMware GUI.

Start

1. Log on to the VMware GUI.
2. Select **Virtual Machines** on the left tab.
3. Click **Register/CreateVM**.
4. Click **Next**.
5. Enter the name. For example, `etcd1`.
6. Select Linux as the **Guest OS Family**.
7. Select Red Hat Enterprise Linux 8 (64-bit) for the **Guest OS Version**.
8. Click **Next**.
9. Select the datastore to which you added the vmdk file. For example, `datastore1`.
10. Click **Next**. The default **Customize Settings** window opens.
11. Customize the VM according to your network requirements.

Customize VMware Settings

On the **Customize Settings** screen, perform the following:

Start

1. Select the **VM Options** tab.
 - a. Click **Boot Options**.
 - b. Select **BIOS** for Firmware.
2. Switch to **Virtual Hardware** tab.
 - a. Delete the default hard drive.

- b. Click **Add Hard Disk**.
 - c. Select **Existing Hard Disk**.
 - d. Select the vmdk file that you previously added to the datastore with the `vmkfstools` command. For example, `AppServices-22.07.00R000-B3500_vmCCS-1.4.1-B2297-x86_64_converted.vmdk`.
 - e. Click **Select** to add the hard drive.
 - f. Change the type of hard drive to **IDE controller 0**.
 - g. Mount the ISO as a CD/DVD drive.
 - h. Under **CD/DVD Drive 1**, select **Datastore ISO file**.
 - i. Select the ISO file that was previously created and copied to the VMware server. For example, `etcd.iso`.
3. Click **Finish** to complete the VM configuration. The newly created VM is listed in the virtual machines tab. For example, `etcd`.
 4. Click on the link for your VM to open the VM status page.
 5. Click the **power on** button to start your VM. The system takes approximately 10 minutes to come up.

Set up the etcd VMs on KVM

To set up etcd on KVM-based VMs, first create an ISO configuration drive.

Create an ISO Configuration Drive for KVM

Complete the following procedure to set up an ISO configuration drive.

Start

1. Log on to the Ribbon Support portal.
2. Download the `AppServices-configDrive.img` and the `AppServices-22.07.00R000-B3500_vmCCS-1.4.1-B2297-x86_64.qcow2` files.
Refer to [Downloading Files from Ribbon Support Portal](#) for information on using the portal.
3. Log on to a Linux server as the root user.
On this server you will create an `.iso` file from the provided template file (`AppServices-configDrive.img`) to use as a configuration drive for the VMs.
4. Create a temporary directory. In the following example the directory name is "etcd."

```
mkdir -p /tmp/etcd
```

5. Mount the image.

```
sudo mount AppServices-configDrive.img /tmp/etcd
```

6. Edit the cloud configuration.

```
vim /tmp/etcd/user-data
```

[Click to view parameter details...](#)

Parameters To Edit	Description	Example	Note
hostname	Hostname of the VM in use	hostname: "amma netcd"	
fqdn	FQDN of the VM in use	fqdn: "ammanetc d.local.com"	
timezone	Choose the time zone	timezone: "Asia/ Kolkata"	
ntp	NTP server IP	servers: ["10.128.254.67"]	
content	Persistent hostname file	write_files: # Persistent hostname file - content: "amman etcd" # Must match 'fqdn' value above	

Parameters To Edit	Description	Example	Note
VnfName GatewayIpv4/ GatewayIpv6 ExternalIp	Name of the VNF as in "ammanetcd" Gateway IP address of the etcd instance IP address of the etcd instance	# Ribbon vmCCS userdata: - content: { "VnfName": "ammanetcd",	◦ Net{1,2,3}: Definition for the interface IF{1,2,3} ◦ Enabled : Indicates if the interface is enabled. Enabled is mandatory. It must be set to "true" or "false". ◦ GatewayIpv4: IPv4 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface ◦ GatewayIpv6: IPv6 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface ◦ ExternalIp: External IP address for this interface ◦ Categories: List of category of traffic on this interface. By default, management is on net1, signaling and internal are on net2, and nothing is configured for net3.

Parameters To Edit	Description	Example	Note
		<pre> "Networks": { "Net1": { "Enabled": "True", "GatewayIpv4": "", "GatewayIpv6": "fd00:10:6b50:40c0 ::1", "ExternalIp": "fd00:10:6b50:40c0 ::24", "Categories": [], "IsDefault": "True" }, "Net2": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "ExternalIp": "", "Categories": [], "IsDefault": "" }, "Net3": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "ExternalIp": "", "Categories": [], "IsDefault": "" } }, </pre>	◦ IsDefault: Indicates whether the default route should be assigned to this interface. Only one interface may have <code>IsDefault=true</code>. If <code>false</code> for all interfaces, the first interface with a gateway configured will be assigned the default route. This parameter is not required if only one gateway was specified in the network-config file.

Parameters To Edit	Description	Example	Note
Etcd	Etcd configuration	<pre> "Etcd": { "ExistingEndpoints" : [], "PersistentDataPath" : "", "PersistentBackupPath" : "", "RootPassword" : "", "UserName" : "", "UserPassword" : "", "ClientCert" : "", "ClientKey" : "", "ClientCaCert" : "", "ServerCert" : "", "ServerKey" : "", "ServerCaCert" : "", "PeerCert" : "", "PeerKey" : "", "PeerCaCert" : "", "HeartbeatInterval" : "", "ElectionTimeout" : "", "BackupDiskMaxUse" : "", "BackupDiskKeepFree" : "", </pre>	◦ PersistentDataPath : Path to the persistent disk to use for Etcd data. The virtio number corresponds to the Etcd data volume ID provided in the deployment. ◦ RootPassword: The Etcd database password for the root user. If left blank, no authentication is enabled on the database. In a HA setup, the passwords must match on all the virtual machines. ◦ UserName: The name of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank. ◦ UserPassword: The password of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank. ◦ HeartbeatInterval: The interval (in ms) at which the leader notifies followers that it is still the leader. The recommended value to set is around the maximum of average round-trip time (RTT) between members, it is normally around 0.5-1.5x the round-trip time. If this field is left blank or omitted, the default value is 100 ms.

Parameters To Edit	Description	Example	Note
		<pre>"BackupStartTime" : "", "BackupFullPeriod" : "0", "BackupRetention" : "" },</pre>	◦ ElectionTimeout: The duration (in ms) that a follower node performs without hearing a heartbeat before attempting to become the leader. The recommended value to set must be at least 10 times the RTT to account for a variance in the network. If this field is left blank or omitted, the default value is 1000 ms. ◦ BackupDiskMaxUse: The maximum percentage of the disk that allowed to be occupied by the Etcd backup files. The default value is 15. ◦ BackupDiskKeepFree : The percentage of disk that must be left free on the file system. The oldest backup files are deleted when this limit is reached. The default value is 30. ◦ BackupStartTime: The time of day when the scheduled backup starts. The format is in hh:mm±hh:mm. The first part of the format is the start time and second part is an offset (from UTC) to specify the time zone. If the time zone is not specified, then the local time zone of the virtual machine processing the request is used as the default time zone. The default value is 02:00.

Parameters To Edit	Description	Example	Note
			◦ BackupFullPeriod : The interval at which a full backup of the Etcd full is performed. This is expressed in the format of weeks and/or days, or hours. For example, 1w2d or 4h. Hours are not allowed to be provided with days or weeks. • The maximum allowed value for hours is 23h. • The minimum allowed value is 1h. • 0 means that no backup is performed. The default value is 1d. Note Set the BackupFullPeriod as 0 (Zero). ◦ BackupRetention : Specifies how long the backup files are retained before deleting the file(s). An empty value means that the backup files are retained for 7 days. This is expressed in the format of weeks, days and/or hours. For example, 1w24h or 2d.

Parameters To Edit	Description	Example	Note
EtcRegistries	IP addresses of any etcd instances created before	"VnfOperations": { "EtcRegistries" : ["10.54.8.166","10.54.8.165"], "EtcUserName": "admin", "EtcUserPassword": "admin", "Salt": "mysalt@123"	While creating the first instance, "EtcRegistries" does not contain any value. While creating the second instance, "EtcRegistries" must contain the IP address of first etcd instance that was created. While creating the third instance, "EtcRegistries" must contain the IP addresses of the first and second etcd instances that were created.
VnfExistingInstances	IP addresses of any etcd instances created before	"VnfExistingInstances" : ["10.54.8.166","10.54.8.165"], "VnfReplaceInstance" : "", "UseMongoDB" : "", "UseEtcd" : "True", "UsePrometheus" : "", "UseAlertManager" : "",	While creating the first instance, "VnfExistingInstances" does not contain any value. While creating the second instance, "VnfExistingInstances" must contain the IP address of first etcd instance that was created. While creating the third instance, "VnfExistingInstances" must contain the IP addresses of the first and second etcd instances that were created.

7. Edit the network configuration:

```
vim /tmp/etcd/network-config
```

Edit the following parameters in the network-config file:

Parameters To Edit	Description	Example
addresses gateway4/ gateway6	IP address to assign to this interface. The default IP gateway.	# DO NOT CHANGE version: 2 # List of network interfaces ethernets: # Network 1 eth0: addresses: # List of IP[v4,v6] addresses to assign to this interface - 10.54.48.60/23 # example: 10.20.30.5/24, fd00:10:6b50:5180::24/60 # Disable if not using IPv4 gateway4: "10.54.48.1" # Default IPv4 gateway, can be moved to another interface if desired (example: default gateway on eth2) # Enable if using IPv6 # gateway6: "" # Default IPv6 gateway, can be moved to another interface if desired (example: default gateway on eth2)

8. Issue the `genisoimage` command to create the ISO file:

```
genisoimage -o etcd.iso -V cidata -r /tmp/etcd
```

9. After creating the ISO file, remove the temporary etcd directory:

```
sudo umount /tmp/etcd  
rm -rf /tmp/etcd
```

The ISO configuration is now complete.

10. Copy the `.iso` file created and the `AppServices-22.07.00R000-B3500_vmCCS-1.4.1-B2297-x86_64.qcow2` to the KVM host.

Create the etcd VMs on a KVM Platform

Complete the following steps to instantiate the etcd VMs on a KVM platform.

Start

1. Install the VNF using `virt-install`.

In the following example command:

`--network` assumes that a bridge called `br0` is the VNF's network interface. If you choose to deploy with two network interfaces, add another `--network` statement with the bridge for the second interface.

The order of `--network` is the same as the order of interfaces in the VM (eth0, eth1, ...).

```
export VNF_NAME=ammanetcd # Replace with your desired VM name

sudo virt-install \
  --name $VNF_NAME \
  --memory 8192 \
  --disk /var/lib/libvirt/images/AppServices-22.07.00R000-B3500_vmCCS-1.4.1-B2297-x86_64.qcow2,device=disk,bus=virtio \
  --disk /var/lib/libvirt/images/etcd.iso,device=disk,bus=virtio,readonly=on \
  --os-type linux \
  --os-variant rhel8.2 \
  --graphics none \
  --network bridge=br0,model=virtio \
  --import
```

Set up etcd VMs on OpenStack

Complete the following steps to instantiate VMs on OpenStack on which you will run etcd.

Start

1. Log on to the Ribbon Support portal.
2. Download the Heat template file (heat_template.yml) and image file (AppServices-22.12.00R000-B4256_vmCCS-1.5.3-x86_64.qcow2). For more information on using the portal, refer to [Downloading Files from Ribbon Support Portal](#).
3. Create or re-use an existing flavor that specifies the recommended configuration (1 vCPU, 2GB of memory, 50GB of disk space). For more information, refer to [Create an OpenStack Flavor](#).
4. Create a security group that defines "allow" rules for the following ingress and egress traffic. For more information, refer to [Create a Security Group](#).

Port	Description
2381	Etcd Prometheus exporter
9013	Nginx Prometheus exporter
9100	Prometheus node exporter (metrics)
9216	MongoDB Prometheus exporter
9292	Backup-manager Prometheus exporter
9090	Prometheus
9093	Prometheus AlertManager client
9801	Service Discovery Representative (SDR) Prometheus exporter
9802	nf-operations exporter

Port	Description
24231	Fluentbit Prometheus exporter
5432	DBaaS replication
6432	DBaaS pgbouncer
5000	DBaaS restapi
27017	MongoDB
9094	Prometheus AlertManager cluster communication
2379	Etcd client requests
2380	Etcd peer communication

5. Configure an external network for your deployment. For more information, refer to [Create an External Network](#).

Name	Description	Default
Public network 1	Public network with floating IP addresses for network 1. Used to allocate a floating IP to the instance.	EXT_OAM_1_DHCP

6. Create a etcd image on the Glance image server using the qcow2 image file you downloaded. For more information, refer to [Create a Glance Image](#).
7. Use the **Launch Stack** window in the OpenStack GUI to launch the etcd instance and update the parameters for your environment.

[Click to view parameter details...](#)

Parameter	Description	Mandatory	Example
image	Image to use for the etcd VM, use the image uploaded in step 5	Yes	AppServices-22.12.00A000-B4225_vmCCS-1.6.0-alpha-B2575-x86_64.qcow2
flavor	OpenStack flavor to use, use the flavor created at step 2	Yes	46fd3493-108e-456d-9c47-66a1ea95d699
security group	Security group to use for the VM, use the security group create at step 3	Yes	default

Parameter	Description	Mandatory	Example
availability zone	Network availability zone for this VNF	No	
management interface hostname	Hostname to use for management interface	No	ammanetcd
management interface domain name	Domain name to use for management interface	No	ammanetcd
user root password	Password for the root user of the VNF instance	No	Sonus@123
user sysadm password	Password for the <code>sysadm</code> user of the VNF instance. (<code>sysadm</code> is the administrative account)	Yes	Sonus@123
Etcd registries	IP addresses of any etcd instances created previously. - While creating the first instance, the "EtcdRegistries" do not contain any value. - While creating the second instance, the "EtcdRegistries" should contain the IP address of first etcd instance that was created. - While creating the third instance, the "EtcdRegistries" should contain the IP address of the first and second etcd instances that were created.	Yes	fd00:10:6b50:61b0::4c7,fd00:10:6b50:61b0::1bc
Existing VNF instances	IP addresses of any etcd instances created previously.	Yes	fd00:10:6b50:61b0::4c7,fd00:10:6b50:61b0::1bc
Etcd username	Name of an etcd user with read/write permissions to all keys related to VNF operations.	Yes	admin

Parameter	Description	Mandatory	Example
Etcd password	Password of for the etcd user with read/write permissions to all keys related to VNF operations.	Yes	admin
Salt	Salt value for cryptography operations accomplished during VNF operations. Ensure the value is identical for all VMs in a deployment and is unique per deployment.	Yes	Sonus@123
Public network 1	Public network with floating IP addresses for network 1. Use to allocate a floating IP to the instance.	Yes	EXT_OAM_1_DHCP
Provide Etcd	Provide Etcd as a service	Yes	true
DNS nameserver(s)	Comma-separated list of DNS nameservers to use in the private subnet	No	fd00:10:6b50:61c0::4d1,f d00:10:6b50:61c0::4d2
DNS search domains	Comma-separated list of DNS search domains to use in the private subnet	No	rbbn.com
NTP server(s)	Comma-separated list of time servers to use for clock synchronization	No	fd00:10:6b50:61c0::4d3
NTP time zone	Time zone used for clock synchronization	No	America/New_York

Health Check etcd

You can check the status of cluster synchronization and health of any node.

Prerequisites

- The etcd is up and running.

Health check on etcd

- Log on as a `root` user.
- Perform a health-check OF the cluster state:

```
root@services3 ~]# /etc/rbbn/appservices/scripts/etcdStatus.py
```

Example output

Name	ID	Endpoint	Leader	Healthy
services1	64386b664d63723b	http://172.29.86.21:2379	false	true
services2	81dcb39d0b4f7142	http://172.29.86.81:2379	true	true
services3	c88e907d0579400a	http://172.29.86.69:2379	false	true

Renew Certificates on VMware and KVM etcd

When a certificate based etcd is deployed with a cnf etcd cluster, renew the certificates.

1. Replace the existing certificates manually. The certificates are available at `/var/lib/rbbn/etcd/certs/`. Replace and retain the same file names.

```
etcd-client.pem
etcd-client-key.pem
etcd-client-ca.pem
etcd-server.pem
etcd-server-key.pem
etcd-server-ca.pem
etcd-peer.pem
etcd-peer-key.pem
etcd-peer-ca.pem
```

2. After manually updating the `.pem` files, apply the changes:

```
systemctl restart etcd
```

RAMP CNF - Observability

In this section:

- [Logging](#)
- [Observability Framework for Log Aggregation](#)
- [Observability Configuration](#)
- [Accessing Logs in Elastic Search Backend Server - Kibana](#)

The Ribbon Application Management Platform (RAMP) Cloud Native Functionality (CNF) application is designed based on Observability (OBS). This design provides comprehensive and real-time visibility into the application's performance and behavior.

Ribbon uses OpenTelemetry to implement the Ribbon Observability Stack and supports selected components from the OpenTelemetry community. The aim is to support all CNF based Ribbon products to enable streaming observability data. With the introduction of this new stack, you can normalize and pre-process all logs and metrics (and in the future, traces) to help correlate and deliver multiple data points captured from each microservice to the configured backends.

Logging

A log is a timestamped text record. Logs are either structured or unstructured, and contain metadata. While logs are independent data sources, they may also get attached to spans. In OpenTelemetry, any data that is not part of a distributed trace or a metric is a log. For example, events are a specific type of log.

Logs are often used to determine the root cause of an issue. They also contain details on who made changes and where, as well as the outcome of the pages.

The RAMP CNF streams the logs from all the microservices and containers to the Observability backend. Examples of Observability backends for centralized logging include EFK and Kafka, among others. The logs given to the Observability backend have a uniform format.

Various formats (with examples) are listed below.

log4jformat

```
Format: <timestamp> <log-level> <Thread-name> <class-name> <method-name> - <message>
```

Example of log4jformat

```
2023-07-06 20:14:07,324 IST INFO [main] SNMPDecodeProcessor <init> -
AvroConverted_TrapProducer Configured Successfully
```

system logs format

```
<timestamp> <hostname> <message>
```

Example of system logs format

```
Eg: "2023-07-06 20:09:20,000 +05:30 sanrampblr-rampcnf-0 sudo[656]:
pam_unix(sudo:session): session closed for user postgres"
```

script logs format

```
<timestamp> <message>
```

Example of script logs format

```
2023-07-06 20:17:23,871 IST fm.converter is online with PID=17096
```

PM python logs format

```
<timestamp> <log-level> <class-name> <message>
```

Example of PM python logs format

```
2023-07-05 13:04:02 IST INFO ClusterHourlyAggregator No stats paths in cluster interval  
parquet folder
```

http access logs format

```
<hostip> - - [timestamp] "<http-method> URL HTTP/1.1" <response-code>
```

An example for http access logs format

Example of http access logs format

```
10.52.80.226 - - [05/Jul/2023:12:12:34 +0530] "GET /auth/v1.0/config/tenant/  
38400000-8cf0-11bd-b23e-10b96e4ef00d HTTP/1.1" 403 13 "-" "Apache-HttpClient/4.5.13  
(Java/1.8.0_372)"
```

Application logs with metadata details added by Observability

Example of application logs with metadata details

```
worker-10.blr-ocp1.lab.rbbn.com.sanrampblr-rampcnf-0.ramp-container.ramp-http-
access.access_log: [1688824469.000000000, {"user":"-", "method":"GET", "code":"200", "size":"
245", "host.geo.timezone":"Asia/Kolkata", "event.original":"10.52.80.2 - - [08/Jul/
2023:19:24:29 +0530] \"GET /auth/v1.0/config/tenant/38400000-8cf0-11bd-b23e-10b96e4ef00d
HTTP/1.1\" 200 245 \"-\" \"Apache-HttpClient/4.5.13 (Java/1.8.0_372)\""}, {"orchestrator.re
source.id":"a3cd296e-4e8b-48c3-b7e3-039087af1b7a", "orchestrator.resource.name":"sanrampb
lr-rampcnf-0", "container":{"runtime":"cri", "labels":{"controller-revision-hash":"sanramp
blr-rampcnf-78ffd88fb9", "element":"rampcnf", "group":"sanrampblr", "servicetype":"observab
ility", "statefulset_kubernetes_io/pod-name":"sanrampblr-rampcnf-0", "tenant":"ramp", "app":"
sanrampblr-rampcnf-pod", "app_kubernetes_io/instance":"sanrampblr", "version":"23.06.00-94
", "component":"prometheus-rbbn-otel-agent"}}, {"referer":"-", "agent":"Apache-HttpClient/
4.5.13 (Java/1.8.0_372)", "log.file.path":"/var/log/logcentral/http/access_log", "orchestr
ator.namespace":"ems-svt", "source.bytes":0, "path":"/auth/v1.0/config/tenant/
38400000-8cf0-11bd-b23e-10b96e4ef00d", "topic":"rampsvt-ramp-systemLogs", "host":"10.52.80
.2", "message":"\"GET /auth/v1.0/config/tenant/38400000-8cf0-11bd-b23e-10b96e4ef00d HTTP/
1.1\" 200 245 \"-\" \"Apache-HttpClient/4.5.13 (Java/1.8.0_372)\""}, {"ecs.version":"1.6.0", "
log.level":"INFO"}]
```

```
worker-10.blr-ocp1.lab.rbbn.com.sanrampblr-rampcnf-0.ramp-container.ramp-log4j-
parser.sftp_collector_application.log: [1688824436.316000000, {"log.level":"INFO", "orche
strator.resource.id":"a3cd296e-4e8b-48c3-b7e3-039087af1b7a", "message":"main: Starting
collector daemon process :: SFTP", "event.original":"2023-07-08 19:23:56,316 IST INFO
[main] StatsCollector main: Starting collector daemon process :: SFTP", "topic":"rampsvt-
ramp-systemLogs", "log.logger":"StatsCollector", "source.bytes":0, "container":{"runtime":"
cri", "labels":{"controller-revision-hash":"sanrampblr-rampcnf-78ffd88fb9", "element":"ram
pcnf", "group":"sanrampblr", "servicetype":"observability", "statefulset_kubernetes_io/pod-
name":"sanrampblr-rampcnf-0", "tenant":"ramp", "app":"sanrampblr-rampcnf-pod", "app_kuberne
tes_io/instance":"sanrampblr", "version":"23.06.00-94", "component":"prometheus-rbbn-otel-
agent"}}, {"process.thread.name":"main", "host.geo.timezone":"Asia/Kolkata", "orchestrator.r
esource.name":"sanrampblr-rampcnf-0", "orchestrator.namespace":"ems-svt", "log.file.path":
"/var/log/logcentral/pm/sftp_collector_application.log", "ecs.version":"1.6.0"}]
```

```
worker-10.blr-ocp1.lab.rbbn.com.sanrampblr-rampcnf-0.ramp-container.ramp-log4j-
parser.ems_trace_log: [1688824507.622000000, {"log.level":"INFO", "orchestrator.resource.
id":"a3cd296e-4e8b-48c3-b7e3-039087af1b7a", "log.logger":"TransactionManagement", "source.
bytes":0, "container":{"runtime":"cri", "labels":{"controller-revision-hash":"sanrampblr-
rampcnf-78ffd88fb9", "element":"rampcnf", "group":"sanrampblr", "servicetype":"observabilit
y", "statefulset_kubernetes_io/pod-name":"sanrampblr-rampcnf-0", "tenant":"ramp", "app":"sa
nrampblr-rampcnf-pod", "app_kubernetes_io/instance":"sanrampblr", "version":"23.06.00-94", "
component":"prometheus-rbbn-otel-agent"}}, {"event.original":"2023-07-08 19:25:07,622 IST
INFO [ServerService Thread Pool -- 79] TransactionManagement - TransactionManagement():
initialized db trap publisher.", "process.thread.name":"ServerService Thread Pool --
79", "orchestrator.resource.name":"sanrampblr-rampcnf-0", "orchestrator.namespace":"ems-
svt", "host.geo.timezone":"Asia/Kolkata", "topic":"rampsvt-ramp-systemLogs", "log.file.path
":"/var/log/logcentral/sys/ems_trace_log", "message":"- TransactionManagement():
initialized db trap publisher.", "ecs.version":"1.6.0"}]
```

Observability Framework for Log Aggregation

In a CNF framework, the logs are aggregated in a centralized backend server. The locally stored logs are lost in the event of a pod restart, crash, or eviction. The observability framework streams the logs to the backend to ensure the logs are accessible even if the pods are not available.

The supported logging mechanisms are:

- Streaming logs to stdout - uses the default Kubernetes logging framework to collect the logs.
- Streaming logs to the backend (Elastic search, for example, Kibana and Kafka).

Observability Configuration

Use the following Helm configuration to configure the observability backend server for logging.

```
logs:
  enable: true
  disablePvcLogs: False # Disables PVC logging
  defaultTopic: default # log messages to this Kafka topic by default when a topic for
the container parsers or system is not specified
  system: true
  systemTopic: system # system logs will be sent to this Kafka topic, defaultTopic is
used if this property is not defined
  telemetry:
    enable: True # Process the otel agent logs
    topic: rbbn-otel-agent # Open telemetry logs will be sent to this Kafka topic
  podlogs: false
  logPrefix:
    nodeId: true
    containerId: false
  # Based on the observability backend server used for logging, uncomment the
elasticserach or kafka
  backendServers: # Example of backend servers. To disable a log backend, provide an
empty array of endpoints, for example: kafka: []
  stdout:
    enable: False # When true, all OBS and app logs are send through STDOUT
  elasticsearch:
    # pick the endpoint based on the location from where you are deploying your CNF
    - endpoint: elasticsearch.apps.blr-ocp1.lab.rbbn.com:443
      auth: True
      username: ELASTICSEARCH_USER
      password: ELASTICSEARCH_PASSWD
      index: platform-filebeat
  kafka: []
  # - endpoint: ip:port
  #   sslCert: KAFKA_CERT
  #   sslKey: KAFKA_KEY
  #   sslCa: KAFKA_CA

# Observability Backend - Elasticsearch Credentials
elasticsearchCreds:
  create: True
  user:
```

```

    key: ELASTICSEARCH_USER
    value:
password:
    key: ELASTICSEARCH_PASSWD
    value:

# Observability Backend - KAFKA Credentials
# all values should be base64 encoded.
kafkaCreds:
  create: False
  #path: /etc/kafka/ssl
  #sslCert:
    #key: KAFKA_CERT
    #value:
  #sslKey:
    #key: KAFKA_KEY
    #value:
  #sslCa:
    #key: KAFKA_CA
    #value:

```

Accessing Logs in Elastic Search Backend Server - Kibana

You can view the exported data to elastic search stack using tools such as Kibana. Kibana is a free and open frontend application that sits on top of the Elastic Stack providing search and data visualization capabilities for data indexed in an Elasticsearch.

On Kibana:

- Use the following query to search whole cluster logs:

```
Query: container.labels.group : "cnfperframp"
```

- Use the following query to search logs based on log file path:

```
Query: orchestrator.resource.name : "cnfperframp-rampcnf-0" and
log.file.path : "/var/log/logcentral/aa/auth_application.log"
```

RAMP CNF - Performance Metrics

In this section:

- [System Metrics](#)
- [Application Metrics](#)

The Ribbon Application Management Platform (RAMP) Cloud Native Functionality (CNF), collects system metrics from CPU, memory, disk read/write, etc, and application metrics from the DSI, GSX, SGX, PSX CNe, and SBC CNe, to monitor the health, operational efficiency, and usage levels. The RAMP Observability forwards the metrics collected from DSI, GSX, and SGX in the Prometheus format. The PSX CNe and SBC CNe statistics are forwarded by the respective devices into the Prometheus format.

System Metrics

RAMP CNF collects system metrics from CPU, memory, disk read/write, and so on using Prometheus query.

A sample of system metric descriptions:

```
# HELP rbbn_container_process_cpu_usage_info_total Per process cpu core usage data in
seconds (sec) since process began
# HELP rbbn_container_process_mem_info Per process memory data in bytes
# HELP rbbn_container_process_disk_info Per process disk data per sec
# HELP rbbn_container_process_page_fault_info_total Per Process page faults since
process began (major faults have loaded a memory page from disk while minor faults have
not)
# HELP rbbn_container_resource_usage The resource usage of a container
# HELP rbbn_container_filesystem_size_info Total storage for given mounting point in
bytes (B)
# HELP rbbn_container_filesystem_used_info Used storage within given mounting point in
bytes (B)
```

A sample of the Prometheus query:

```
rbbn_container_process_cpu_usage_info_total{orchestrator_namespace="ems-
svt",k8s_pod_name="sanrampblr-rampcnf-0",process_name="pgbouncer"}
```

Application Metrics

RAMP CNF collects metrics from the registered DSI, GSX, and SGX devices using the Prometheus format. This data is then scraped through by Observability at configured intervals. For more information on Observability, refer to [RAMP CNF - Observability](#).

A sample Prometheus query:

```
rbbn_pmIntervalStats_TIME_LINK_DOWN_REASON_FAIL{NODE_ID="SGXCNF",k8s_pod_name="sanrampbl
r-rampcnf-0",tenant="ramp",service_name="pm-stats"}
```

Installation and Upgrade Guide

This section provides installation procedures for the Ribbon Application Management Platform (RAMP) on a variety of platforms.

In this section:

- [Installing RAMP](#)
 - [Hostname and Instance Name Conventions](#)
 - [Installing RAMP in Virtual and Private Cloud Environments](#)
 - [Installing RAMP in Public Cloud Environments](#)
 - [Installing RAMP CNF](#)
 - [Install and Configure Ribbon OEM Host OS for RAMP on Dell Server](#)
 - [RAMP Customization for Docker Daemon](#)
- [Upgrading RAMP](#)
 - [Pre-Upgrade Checklist](#)
 - [Upgrading RAMP in Virtual and Private Cloud Environments](#)
 - [Upgrading RAMP in Public Cloud Environments](#)
 - [Upgrading RAMP CNF](#)
 - [Post-Upgrade Procedures for RAMP](#)
- [Migrating to RAMP](#)
 - [Migrate EdgeView to RAMP](#)
 - [Migrate Insight EMS to RAMP](#)
- [Installing etcd](#)
 - [Installing etcd on Kubernetes](#)
 - [Installing etcd on KVM](#)
 - [Installing etcd on OpenStack](#)
 - [Installing etcd on VMware](#)
- [Upgrading etcd](#)
 - [Upgrading etcd on KVM](#)
 - [Upgrading etcd on VMware](#)
 - [Upgrading etcd on Openstack](#)
 - [Upgrading etcd on Kubernetes](#)
- [Health Check etcd](#)
- [Rolling Back RAMP CNF](#)
- [Uninstalling RAMP CNF](#)
 - [RAMP CNF - Uninstall Using Git](#)
 - [RAMP CNF - Uninstall Using Helm Commands](#)
 - [RAMP CNF - Delete PVCs](#)

Installing RAMP

Contents

- [Hostname and Instance Name Conventions](#)
 - [Change the Hostname of a StandAlone RAMP](#)

- [Installing RAMP in Virtual and Private Cloud Environments](#)
 - [Installing RAMP on KVM Manually](#)
 - [Installing RAMP on OpenStack](#)
 - [Installing RAMP on VMware Manually](#)
- [Installing RAMP in Public Cloud Environments](#)
 - [Installing RAMP on AWS Manually](#)
 - [Installing RAMP on Azure Manually](#)
- [Installing RAMP CNF](#)
 - [RAMP CNF - Standalone Deployment Using GitOps](#)
 - [RAMP CNF - Standalone Deployment Using Helm Charts](#)
 - [RAMP CNF - Post Installation Steps](#)
 - [Generate Certificate Authority](#)
- [Install and Configure Ribbon OEM Host OS for RAMP on Dell Server](#)
- [RAMP Customization for Docker Daemon](#)

Hostname and Instance Name Conventions

Conventions used on this page:

✓ supported

✗ not supported

The following table lists host name conventions to follow while configuring Ribbon Application Management Platform (RAMP). You can provide a name to an instance only while instantiating. The maximum number of characters in a hostname is 63.

Hostname Conventions

Convention/Character	System Name	Use as Leading Character	Use as Trailing Character
Letters [a-z] [A-Z]	✓	✓	✓
Digits [0-9]	✓	✗	✓
Hyphen [-]	✓	✗	✗
Period [.]	✗	✗	✗
Underscore [_]	✗	✗	✗
Other special characters	✗	✗	✗

Change the Hostname of a StandAlone RAMP

Use the following procedure to change the hostname of a StandAlone (SA) Ribbon Application Management Platform (RAMP) instance.

Note

If you registered a cloud-based PSX in RAMP, manually update the new hostname in `/export/home/ssuser/.ssh/authorized_keys` to prevent failures of future PSX node discoveries.

Perform the following procedure to change the hostname of a SA RAMP:

Start

1. Log on to the RAMP CLI as `root`. Refer to [Log onto the RAMP CLI](#).
2. Navigate to the `conf` directory:

```
cd /opt/sonus/ems/conf/
```

3. Change the hostname:

```
./changeHostname.sh <newhostname>
```

Installing RAMP in Virtual and Private Cloud Environments

In this section:

- [Installing RAMP on KVM Manually](#)
 - [Check KVM Host System Requirements](#)
 - [Checklist for Installing RAMP on KVM](#)
 - [Download Files for RAMP Installation on KVM](#)
 - [Update the Configuration File](#)
 - [Resize the QCOW2 Disk Size](#)
 - [Create a RAMP Instance on KVM Using the QCOW2 Image](#)
 - [Download Files for etcd Installation on KVM](#)
- [Installing RAMP on OpenStack](#)
 - [Checklist for Installing RAMP on OpenStack](#)
 - [Add Non-Default Users Using the RAMP Heat Template](#)
 - [Validate the Downloaded QCOW2 File](#)
 - [Create an OpenStack Flavor](#)
 - [Create a Security Group](#)
 - [Create an External Network](#)
 - [Create a Glance Image](#)
 - [Create a Cinder Volume](#)
 - [Generate an Encrypted Password for the RAMP Admin Account](#)
 - [Generate SSH Keys for RAMP Users](#)
 - [SSH to RAMP using SSH Keys](#)
 - [Copy SSH Keys to Instantiate a RAMP Standby Instance](#)
 - [Instantiate RAMP on OpenStack](#)
 - [Instantiating and Managing RAMP using VNFM](#)

- [Post-RAMP Instantiation Tasks](#)
- [Installing RAMP on VMware Manually](#)
 - [Checklist for Installing RAMP on VMware](#)
 - [Install RAMP on VMware](#)
 - [Install RAMP with VMware OVA Template Customization](#)
 - [VMotion on VMware for RAMP](#)

Installing RAMP on KVM Manually

You can install the Ribbon Application Management Platform (RAMP) on KVM (Kernel Virtual Machine) manually using the procedures outlined in this topic. The workflow below provides an overview of the process and provides links to the specific information and steps required to complete installation. After completing the steps on a linked page, return to the workflow for the next procedure.

Step	Action
1	Review System Requirements to ensure your environment has the necessary resources and prerequisite software available
2	Complete steps to verify that the KVM host environment meets the requirements. For more information, refer to Check KVM Host System Requirements .
3	Review the Checklist for Installing RAMP on KVM to ensure you have the network parameters required for the installation process
4	Download the installation files. For more information, refer to Download Files for RAMP Installation on KVM .
5	Update the configuration file for your specific deployment. For more information, refer to Update the Configuration File .
6	You can resize the disk size to a larger size. For more information, refer to Resize the QCOW2 Disk Size .
7	Create a RAMP virtual machine instance. For more information, refer to Create a RAMP Instance on KVM Using the QCOW2 Image .
8	(Optional) If you plan to manage SBC Edge devices with RAMP, enable the EdgeView (EV) service. For more information, refer to Deploy Optional Services on RAMP .

Step	Action
9	(Optional) To configure RAMP in a GR deployment, create a second virtual machine instance to act as the standby node in the GR pair. Create the second instance following a similar process you just completed to create the initial instance. When creating additional instances, use another copy of the qcow2 file, a different mount directory, and another instance of the <code>configDriveImgDeployment.img</code> file. After creating the second instance, refer to Configuring RAMP GR or Configuring RAMP GR with Automatic Switchover Enabled for the procedure to configure the two instances as a GR pair.
10	Install RAMP licenses. For more information, refer to License Management .

After completing installation, refer to the [RAMP User Guide](#) for additional information on configuring and working with RAMP.

Check KVM Host System Requirements

Use the Hostchecker utility to check the system requirements on the KVM host server before installing Ribbon Application Management Platform (RAMP) on KVM. The Hostchecker utility uses the flavor definition in a YAML file provided by Ribbon to run checks on the host server. The flavor definition files for the RAMP flavors are available in the `ramp-hostcheck-Vxx.xx.xxRxxx.tar` file.

The utility checks if the host server meets the minimum RAMP requirements in the following categories. For more information, refer to [System Requirements](#).

Product (flavor)
Kernel Version
Libvirt Version
Qemu Version
Cores
Frequency
Socket(s)
Thread(s)
Hyper-Threading
Total Memory (GB)
Total Disk (GB)

NICs

Install and Run the Hostchecker

Perform the following procedure to install and run the Hostchecker:

Start

1. Download the `ramp-hostcheck-Vxx.xx.xxRxxx.tar.gz` file from the [Ribbon Support Portal](#) to your host server.
2. Navigate to the directory in which the `ramp-hostcheck-Vxx.xx.xxRxxx.tar.gz` file is downloaded.
3. Extract the files:

```
tar -xvf ramp-hostcheck-Vxx.xx.xxRxxx.tar.gz
```

4. Run the utility:

```
./Hostchecker --input <RAMP flavor definition file>
```

Example output

```
./Hostchecker --input ramp_host_checker_large_standalone_swe.yml
```

- If FINAL OUTCOME shows as SUPPORTED, the host server meets the requirements to install the RAMP.
- If FINAL OUTCOME shows as NOT SUPPORTED, the host server does not meet the requirements to install the RAMP. Modify your host server settings for the requirements displayed as "Not Supported" and "Not Validated."

Checklist for Installing RAMP on KVM

Use the following table to assist you in gathering system information in preparation for installing Ribbon Application Management Platform (RAMP) on KVM. Ribbon recommends that you record these parameter values and have them available to use during the installation process and while configuring RAMP.

Installation Parameters for RAMP

Ribbon Network Configuration	Parameter	Description	Example Value	Mandatory
Hostname	Hostname	Specifies a name for the system.	BLRRAMP01a	Yes
IP Configuration	Bridge	Specifies the name of the bridge created in the KVM host.	br0	Yes

Ribbon Network Configuration	Parameter	Description	Example Value	Mandatory
	IP Address	Specifies the IP address for the selected network interface.	10.54.8.62	Yes
	Netmask	Specifies the network mask.	255.255.255.0	Yes
	Gateway	Specifies the gateway IP address of the network.	10.54.8.1	Yes
Time Zone	<code>timeZone</code>	Specifies the time zone for the deployment.	America/New York	Yes
Time Server	<code>ntpServerIpaddr</code>	Specifies the NTP server IP address with which to synchronize the system time.	10.128.245.36	Yes

For hostname conventions, refer to [Hostname and Instance Name Conventions](#).

Download Files for RAMP Installation on KVM

To install the Ribbon Application Management Platform (RAMP) on KVM (Kernel Virtual Machine) manually, download the necessary files using the following procedure:

Create the folder in the partition with a minimum disk size of 300GB. Copy the QCOW2 to this partition and resize it.

Start

Use the following procedure to download the [RAMP](#) installation files:

1. Create a download directory **on the host system**:

```
mkdir -p <path>
```

Example:

```
mkdir -p /var/lib/libvirt/images/
```

2. Configure the `images` directory to have all the permissions:

```
chmod 777 /var/lib/libvirt/images/
```

3. Log on to the Ribbon Support Portal to download the files. Refer to [Download Files from Ribbon Support Portal](#).
4. Download the following files to the `/var/lib/libvirt/images` directory:
 - `ramp-V<version>-RHEL-<version>-x86_64_68.qcow2`
 - `configDriveImgDeployment.img`

Note

In the process of creating the VM, the image is converted to a disc image for the VM. You cannot use the image to deploy an instance a second time.

To maintain a copy, create a copy of the QCOW2 file in the same location (with a different name).

5. Return to the workflow table on [Installing RAMP on KVM Manually](#).

Update the Configuration File

Complete the following procedure to update the configuration file with the values to deploy an instance of the Ribbon Application Management Platform (RAMP) on Kernel Virtual Machine (KVM).

Start

1. Log on to the KVM host as the `root` user.
2. Navigate to the directory in which the `qcow2` and `configDriveImgDeployment.img` files were downloaded.
3. Create a temporary mount directory:

Example:

```
mkdir -p /tmp/vmconf
```

4. Mount the `configDriveImgDeployment.img` file in the temporary mount directory:

```
mount -o loop configDriveImgDeployment.img /tmp/vmconf
```

Note

To create multiple instances, use a different mount directory and `configDriveImgDeployment.img` file for each instance.

5. Modify the `configDriveImgDeployment.img` file for your deployment:

```
vim /tmp/vmconf/user-data
```

user-data Parameter Descriptions

Key Name	Description	Example Value	M/O
timezone	The time zone for your network in which the VM is created.	Asia/Kolkata	M
ntpServer	The NTP server IP address if you have an NTP server. To add multiple NTP servers (up to 5 allowed), enter the NTP server IP addresses in the following format: <pre>servers: - \$ntpServer1 - \$ntpServer2 - \$ntpServer3 - \$ntpServer4 - \$ntpServer5</pre>	servers: - 10.128.254.67 - 10.128.254.68 - 10.10.211.119	M
dnsServer	The IP address of the DNS server.	◦ IPV4: 10.128.254.67 ◦ IPV6: 0:0:0:0:ffff:c0a8:101	O
dnsSearchPath	The search path for the DNS server.	rbbn.com	O
InstanceName	The RAMP instance or virtual machine (VM) name. The InstanceName criteria: ◦ Uppercase or lowercase letters [a-z], [A-Z] ◦ Digits [0-9] ◦ Do not begin the name with a digit. ◦ Do not use special characters, including the underscore.	ramp SA	M
instance-type	The RAMP installed on the non-cloud (KVM/VMware).	non-cloud	M

Key Name	Description	Example Value	M/O
MGT1	Note: This flag is set to N. To use the Secondary MGT Interface, change it to Y. If MGT1 is configured, you cannot configure Lawful Interface (LI). By default, MGT1 is set to N. When MGT1 is mandatory, or the flag is set to Y, the IF2 values get populated.	Y	O
IF1		IF1	
GWV4	Note: This parameter is applicable only if you are creating a RAMP VM in an IPv4 network. The gateway IP address from the available network pool in IPv4. "1" indicates the interface number.	192.168.1.1	M
IPV4	Note: This parameter is applicable only if you are creating a RAMP VM in an IPv4 network. The fixed management IPv4 address for the interface. IF1Ipaddr is the IP address of eth0.	192.168.1.7/24	M
GWV6	Note: This parameter is Mandatory if the RAMP uses IPv6. The gateway IP address from the available network pool in IPv6. "101" indicates the interface number.	0:0:0:0:ffff:c0a8:101	O/M
IPV6	Note: This parameter is mandatory if the RAMP uses IPv6. The fixed management IPv6 address for the interface and netmask. IF1Ipaddrv6 is the IP address of eth0.	0:0:0:0:ffff:c0a8:107/64	O/M

Key Name	Description	Example Value	M/O
IF2		IF2	
GWV4	Note: This parameter is applicable only if you are creating a RAMP VM in an IPv4 network. The gateway IP address from the available network pool in IPv4.	192.168.1.1	M
IPV4	Note: This parameter is mandatory if you are creating a RAMP VM in an IPv4 network. The fixed management IPV4 address for the interface. ◦ IF2Ipaddr is the IP address of eth1.	182.168.1.7/24	M
GWV6	Note: This parameter is mandatory if RAMP uses IPv6. The gateway IP address from the available network pool in IPv6. "101" indicates the interface number.	0:0:0:0:ffff:c0a8:101	O/M
IPV6	Note: This parameter is mandatory if RAMP uses IPv6. The fixed management IPv6 address for the interface and netmask. ◦ IF2paddrv6 is the IP address of eth1.	0:0:0:0:ffff:c0a8:107/64	O/M

Example:

```

path: /opt/rbbn/userData.json
permissions: '0644'
content: |
{
  "IF1": {"GWV4": "$gwv4", "IPV4": "$ip4/$prefix", "Port": "eth0"},
  "IF2": {"GWV4": "", "IPV4": "/", "Port": ""},
  "growpart": { "opt" : 60, "pgsql": 30, "home": 10},
  "instance-type": "non-cloud",
  "InstanceName": "$instanceName",
  "MGT1": "N" # Make it "Y" when using Secondary MGT Interface
}

```

If MGT1 is set to Y:

```

path: /opt/rbbn/userData.json
permissions: '0644'
content: |
{
  "IF1": {"GWV4": "$gwv4", "IPV4": "$ipv4/$prefix", "Port": "eth0"},
  "IF2": {"GWV4": "$gwv4", "IPV4": "$ipv4/$prefix", "Port": "eth1"},
  "growpart": { "opt" : 60, "pgsql": 30, "home":10},
  "instance-type": "non-cloud",
  "InstanceName": "venus2ramp",
  "MGT1": "Y"
}

```

6. If your internal network clashes with the networks created by the docker service, add the file `/opt/rbbn/dockerNetworksFile` through the user-data or the HEAT template. This file validates and writes the data to the `/etc/docker/daemon.json` file. For more information on Docker Daemon, refer to [RAMP Customization for Docker Daemon](#).

Note

At times, the internal network assigned by the docker service is the same as the network used in your premises. This leads to a conflict in the network and connectivity issues. In such a scenario, specify the docker service to pick the provided IP Address from the pool for the docker internal network.

Note

You must add a minimum of seven networks for the RAMP 24.06 release. You are allowed to add networks that suit you, but do not change the variable names.

IPV6 support is currently disabled.

Example code

```

write_files:
- path: /opt/rbbn/dockerNetworksFile
permissions: '0744'
owner: root:root
content: |
  dockerNetwork1=172.21.0.0/16
  dockerNetworkSize1=24
  dockerNetwork2=172.22.0.0/16
  dockerNetworkSize2=24
  dockerNetwork3=172.23.0.0/16

```

```

dockerNetworkSize3=24
dockerNetwork4=172.24.0.0/16
dockerNetworkSize4=24
dockerNetwork5=172.25.0.0/16
dockerNetworkSize5=24
dockerNetwork6=172.26.0.0/16
dockerNetworkSize6=24
dockerNetwork7=172.27.0.0/16
dockerNetworkSize7=24

```

Example: Created user data

```

#cloud-config
timezone: "Asia/Kolkata"
ntp:
  enabled: true
  ntp_client: chrony
  config:
    conffpath: /etc/chrony.conf
    check_exe: chronyd
    packages:
      - chrony
    service_name: chronyd
    template: |
      ## template:jinja
      # My NTP Client config
      {%- if servers %}# servers
      {% endif %}
      {% for server in servers -%}
      server {{server}} iburst
      {% endfor %}
    servers:
      - 10.128.254.68
manage_resolv_conf: true
resolv_conf:
  nameservers: ['8.8.8.8']
  searchdomains:
    - $dnsSearchPath
write_files:
  - path: /opt/rbbn/userData.json
    permissions: '0644'
    content: |
      {
        "IF1": {"GWV4": "10.220.200.2", "IPV4": "10.220.200.168/24", "Port": "eth0"},
        "growpart": { "opt" : 60, "pgsql": 30, "home":10},
        "instance-type": "non-cloud",
        "InstanceName": "RAMP01"
        "MGT1": "N"
      }
owner: root:root

```

```

- path: /opt/rbbn/dockerNetworksFile
  permissions: '0777'
  content: |
    dockerNetwork1=172.21.0.0/16
    dockerNetworkSize1=24
    dockerNetwork2=172.22.0.0/16
    dockerNetworkSize2=24
    dockerNetwork3=172.23.0.0/16
    dockerNetworkSize3=24
    dockerNetwork4=172.24.0.0/16
    dockerNetworkSize4=24
    dockerNetwork5=172.25.0.0/16
    dockerNetworkSize5=24
    dockerNetwork6=172.26.0.0/16
    dockerNetworkSize6=24
    dockerNetwork7=172.27.0.0/16
    dockerNetworkSize7=24
  owner: root:root
runcmd:
- usermod -p '$1$admin$1kgWpnZpUx.vTroWPXPIB0' admin
- usermod -f -1 admin

```

An example of IPv6 inputs/when MGT1 is set to Y:

```

[root@venus1 IPV6]# cat /tmp/vivek/user-data
#cloud-config
timezone: "Asia/Kolkata"
ntp:
  enabled: true
  ntp_client: chrony
  config:
    conffpath: /etc/chrony.conf
    check_exe: chronyd
    packages:
      - chrony
    service_name: chronyd
    template: |
      ## template:jinja
      # My NTP Client config
      {%- if servers %}# servers
      {% endif %}
      {% for server in servers -%}
      server {{server}} iburst
      {% endfor %}
  servers:
    - 10.128.254.67
    - $ntpServer2
    - $ntpServer3

```

```

- $ntpServer4
- $ntpServer5
manage_resolv_conf: true
resolv_conf:
  nameservers:
    - $dnsServer1
    - $dnsServer2
  searchdomains:
    - $dnsSearchPath
write_files:
- path: /opt/rbbn/userData.json
  permissions: '0644'
  content: |
    {
      "IF1": {"GWV6": "fd00:10:6b50:48d0::1", "IPV6": "fd00:10:6b50:48d0::49/60", "
Port": "eth0"},
      "IF2": {"GWV6": "fd00:10:6b50:40c0::1", "IPV6": "fd00:10:6b50:40c0::a2/60", "
Port": "eth1"},
      "growpart": { "opt" : 60, "pgsql": 30, "home":10},
      "instance-type": "non-cloud",
      "InstanceName": "venus1rampipv6",
      "MGT1": "Y"
    }
  owner: root:root
# Make "MGT1": "Y" when using Secondary MGT Interface
# Uncomment if user needs specific ip range to be used for docker networks. Ref
AFM-10888
# more details can be found on wiki about docker d,aemon customisation
# IPs can be edited but each one of them should be valid and unique.

# - path: /opt/rbbn/dockerNetworksFile
# permissions: '0744'
# owner: root:root
# content: |
#   dockerNetwork1=172.21.0.0/16
#   dockerNetworkSize1=24
#   dockerNetwork2=172.22.0.0/16
#   dockerNetworkSize2=24
#   dockerNetwork3=172.23.0.0/16
#   dockerNetworkSize3=24
#   dockerNetwork4=172.24.0.0/16
#   dockerNetworkSize4=24
#   dockerNetwork5=172.25.0.0/16
#   dockerNetworkSize5=24
#   dockerNetwork6=172.26.0.0/16
#   dockerNetworkSize6=24
#   dockerNetwork7=172.27.0.0/16
#   dockerNetworkSize7=24
runcmd:
- usermod -p '$1$admin$1kgWpnZpUx.vTroWPXPIB0' admin
- usermod -f -1 admin

```

7. Save and close the configuration file.
8. Unmount the image:

```
umount /tmp/vmconf
```

9. Delete the temporary mount point:

```
rm -rf /tmp/vmconf
```

10. Return to the workflow table on [Installing RAMP on KVM Manually](#).

Resize the QCOW2 Disk Size

Complete the following procedure to increase the virtual disk size of the qcow2 image file to accommodate a larger deployment. By default, the qcow2 image provides a disk size that is the minimum disk size (HDD) Ribbon Application Management Platform (RAMP) supports. You can resize the disk based on the resource size that your deployment requires.

For example, to increase the RAMP VM to 900GB, resize the qcow2 file by adding 770GB to the initial minimum size (130 GB).

To increase the virtual disk size of the qcow2 image:

1. Check the disk size of the qcow2 image using the following command:

```
qemu-img info <Absolute qcow2 Image path> | grep "virtual size"
```

The following is an example:

```
qemu-img info /home/images/ramp-V24.xx.xxRxxx-RHEL-8.x.xx-x86_64_68.qcow2 | grep "virtual size"
```

2. Increase the disk size by providing the difference between the required size and the initial disk size of the qcow2 image found in the first step:

```
qemu-img resize <Absolute qcow2 Image path> +<disk size>
```

The following is an example:

```
qemu-img resize /home/images/ramp-V24.xx.xxRxxx-RHEL-8.x.xx-x86_64_68.qcow2 +770G
```

The increased additional space is added to /(root).

Note

Run this command only once. If you run the command twice, the sizing is done twice. Resizing to shrink the space is not supported.

3. Validate whether the disk size of the qcow2 image is increased:

```
qemu-img info <Absolute qcow2 Image path> | grep "virtual size"
```

The following is an example:

```
qemu-img info /home/images/ramp-V24.xx.xxRxxx-RHEL-8.x.xx-x86_64_68.qcow2 | grep "virtual size"
```

The following is the output:

```
virtual size: 900G (966367641600 bytes)
```

4. Return to the workflow table on [Installing RAMP on KVM Manually](#).

Create a RAMP Instance on KVM Using the QCOW2 Image

Complete the following steps to create a Ribbon Application Management Platform (RAMP) instance on KVM (Kernel Virtual Machine). If you have not already done so, refer to [Installing RAMP on KVM Manually](#) for a workflow table that outlines the full installation process, including prerequisite steps to review system requirements, gather installation parameters, and download installation files.

In the procedure, the parameter "bridge" refers to the name of the network bridge created on the KVM host. Note that if you copy and paste the commands, the indentation may differ.

1. SSH to the KVM host as the root user.
2. Perform one of the following depending on whether you want a single or multiple network interfaces:
 - a. Create a RAMP instance with a single network interface:

```
/usr/bin/virt-install --name <Name of the VM> --ram <RAM> \
--vcpus sockets=<# of sockets>,cores=<# of cores>,threads=<# of threads> --disk
<Qcow2 absolute path> \
--disk path=configDriveImgDeployment.img,device=disk,cache=none --import --
autostart \
--os-type=linux --os-variant=rhel8.4 --arch=x86_64 \
--network type=<network type>,source=<source>,model=<model> \
--noautoconsole
```

Check the RHEL OS variant using the following command on the KVM host machine:

```
osinfo-query os | grep -i 'Red Hat' | sort -n | tail -1
```

Based on the version displayed, use that version.

Example output:

```
/usr/bin/virt-install --name venus3ramp --ram 65536 --vcpus sockets=1,cores=8,threads=2
--disk /var/lib/libvirt/images/venus3ramp/ramp-V24.09.00A001-RHEL-8.10.96-173-x86_64_529.qcow2
--disk path=/var/lib/libvirt/images/venus3ramp/configDriveImgDeployment.img,device=disk,cache=none --import --autostart
--os-type=linux --os-variant=rhel8.4 --arch=x86_64
--network type=bridge,source=br0,model=virtio
--noautoconsole
```

- b. Create a RAMP instance with multiple network interfaces:

```
/usr/bin/virt-install --name <Name of the VM> --ram <RAM> \
--vcpus sockets=<# of sockets>,cores=<# of cores>,threads=<# of threads> --disk
<Qcow2 absolute path> \
--disk path=configDriveImgDeployment.img,device=disk,cache=none --import --
autostart \
--os-type=linux --os-variant=rhel8.4 --arch=x86_64 \
--network type=bridge,source=<source>,model=<model> \
--network type=bridge,source=<source>,model=<model> \
--noautoconsole
```

Example output:

```
/usr/bin/virt-install --name RAMPsa --ram 65536 \
--vcpus sockets=1,cores=8,threads=2 \
--disk /home/RAMPsa/ramp-V22.06.00R000-RHEL-8.5.20-x86_64_68.qcow2 \
--disk path=/home/RAMPsa/configDriveImgDeployment.img,device=disk,cache=none
--import --autostart \
--os-type=linux --os-variant=rhel8.4 --arch=x86_64 \
--network type=bridge,source=br0,model=virtio \
--network type=bridge,source=br1,model=virtio \
--noautoconsole
```

3. Check the status of the VM instance using the following command:

```
virsh list
```

Example output:

Id	Name	State


```
-----
4      RAMPsa                                running
```

Note

Validate the VM name and ensure that the VM state appears as "running".

4. SSH to RAMP as the admin user.

The default admin password is "admin". To change the password, refer to [Change Linux Admin User Password on RAMP Standalone](#) or [Change Linux Admin User Password on RAMP GR](#).

5. Check the RAMP status. Refer to [Check RAMP Status](#).
6. Return to the workflow table on [Installing RAMP on KVM Manually](#).

Download Files for etcd Installation on KVM

To install the etcd on KVM (Kernel Virtual Machine) manually, download the necessary files using the following procedure:

Create the folder in the partition with a minimum disk size of 300 GB. Copy the QCOW2 to this partition and resize it.

Start

Use the following procedure to download the etcd installation files:

1. Create a download directory on the host system:

```
mkdir -p <path>
```

Example:

```
mkdir -p /var/lib/libvirt/images/
```

2. Configure the `images` directory to have all the permissions:

```
chmod 777 /var/lib/libvirt/images/
```

3. Log onto the Ribbon Support Portal to download the files. Refer to [Download Files from Ribbon Support Portal](#).

4. Download the following files to the `/var/lib/libvirt/images` directory:
 - `AppServices-<version>-<version>_vmCCS-<version>-x86_64.qcow2`
 - `AppServices-configDrive.img`

Note

During the process of creating the VM, the image is converted to a disc image for the VM. Thus, you cannot reuse the image to deploy another instance.

To overcome this, create a copy of the QCOW2 file in the same location, but with a different name.

Installing RAMP on OpenStack

You can install Ribbon Application Management Platform (RAMP) on OpenStack using the procedures outlined in this topic.

The workflow below provides an overview of the process and provides links to the specific information and steps required to complete installation. After completing the steps on a linked page, return to the workflow for the next procedure.

Step	Action
1	Review the Checklist for Installing RAMP on OpenStack to ensure your environment is prepared and that you have the information needed to instantiate RAMP on OpenStack.
2	Create an OpenStack flavor with the necessary RAM, disk size, and vCPU details for your deployment. Refer to Creating an OpenStack Flavor. If you already have an OpenStack flavor with the recommended configuration, you can reuse it.
3	Create a security group and define allow and deny traffic rules for ingress and egress traffic. Refer to Creating Security Group. If you already have a security group defined with the correct allow/deny rules for ingress and egress traffic, you can reuse the existing security group.

Step	Action
4	Configure an external network for your deployment. Refer to Defining Network Configuration. If you already have defined an external network, you can reuse the existing network configuration.
5	Create a RAMP image on the Glance image server. Refer to Create a Glance Image .
6	Create a Cinder volume for your deployment to use as a persistent datastore. Refer to Create a Cinder Volume. If you have an existing cinder volume of an appropriate size that is not attached to any RAMP instance, you can use that volume. Note If you plan to configure a geographically redundant (GR) deployment, create two cinder volumes.
7	Generate a password for the admin account that is in an encrypted format. Refer to Generate an Encrypted Password for the RAMP Admin Account .
8	Generate SSH keys for the RAMP instance. Refer to Generate SSH Keys for RAMP Users .
9	Instantiate the RAMP instance. Refer to Instantiate RAMP on OpenStack .
10	(Optional) If you plan to manage SBC Edge devices with RAMP, enable the EdgeView (EV) service. Refer to Deploy Optional Services on RAMP .
11	(Optional) To deploy RAMP in a GR configuration: 1. You must modify the template to add GR parameters. Refer to Checklist for Installing RAMP on OpenStack. Use the initial instance as the active node. 2. Copy the SSH keys of the active RAMP. Refer to Copy SSH Keys to Instantiate a RAMP Standby Instance. 3. Instantiate a RAMP instance as the standby node. Refer to Instantiate RAMP on OpenStack. 4. Configure Georedundancy parameters. Refer to Configuring RAMP Redundancy.

Step	Action
12	Take a backup of SSH keys and copy them to a server that is external to the RAMP instance. Refer to Obtain the RAMP SSH Keys. For GR deployments, repeat this step for the RAMP standby node.
13	Install RAMP licenses. Refer to License Management .

Refer to [Manage Resources for RAMP on OpenStack](#) for additional procedures specific to administering an OpenStack deployment.

Checklist for Installing RAMP on OpenStack

This topic provides information on how to set up the required OpenStack environment before launching a Ribbon Application Management Platform (RAMP) instance. Environment setup is a one-time activity; once the environment is set up, one or several RAMP instances can be launched.

The checklist consists of setup tasks to complete and values to gather before you instantiate an instance of RAMP on OpenStack. Review the full checklist before you begin. Ribbon recommends that you make a record of the parameter values that you need to enter during the instantiation process and while configuring RAMP.

The checklist table includes example values for parameters. When instantiating your instance of RAMP, use values that are appropriate for your deployment.

Note

The `/etc/hosts` files are updated as part of RAMP instantiation. You must not modify the `hosts` file. Modifying the `hosts` file can result in license issues. Contact Ribbon Global Product Support (GPS) before you make any changes to the `hosts` files.

OpenStack Pre-installation Checklist

Parameter	Description	Example Values	Mandatory?
Prerequisites to Use the OpenStack GUI Dashboard			
OpenStack Dashboard GUI URL	To access the OpenStack GUI dashboard on the controller, type the URL in browser.	<code>http://<controller-IP>/dashboard</code> Replace the <code><controller-IP></code> with your IP address, for example: <code>http://10.54.27.112/dashboard/</code>	Yes

Parameter	Description	Example Values	Mandatory?
OpenStack Dashboard GUI login credentials	The username and password to access the OpenStack GUI dashboard.	username: admin password: admin	Yes
OpenStack CLI Prerequisites			
Set environment variables in the <code>admin-openrc.sh</code> environment file.	Create an environment file <code>admin-openrc.sh</code> and set the environment variables with values clients will use to access the OpenStack command-line. The mandatory environment variables which must be configured are: OS_USERNAME OS_PASSWORD OS_TENANT_NAME OS_AUTH_URL	OS_USERNAME=admin OS_PASSWORD=admin OS_TENANT_NAME=admin OS_AUTH_URL=http://10.54.27.112:35357/v2.0	Yes
Run a script to source the environment file	To put the environment variable changes into effect and allow execution of the OpenStack CLI, you must source the <code>admin-openrc.sh</code> file.	Example: source admin-openrc.sh	Yes
Common Prerequisites			
External Network Name	The name assigned to the external network for the deployment.	ext-net	Yes
External network Subnet Name	The name assigned to the subnet on the external network.	ext-netsubnet	Yes
External Network IP Address	The external routable IP address of the external network.	10.9.9.97	Yes

Parameter	Description	Example Values	Mandatory?
Download the RAMP qcow2 image from the Ribbon Support Portal.	The RAMP qcow2 image package for OpenStack.	ramp-V22.06.00R00-RHEL-8.5.20-x86_64_68.qcow2 Refer to the release notes for the exact file name. Refer to Validate the Downloaded QCOW2 File for a procedure to verify the downloaded file before installation.	Yes
Download RAMP Heat templates	The Heat templates to instantiate RAMP instances.	RAMP_HEAT_TEMPLATE.yaml	Yes
Add additional users	Refer to Add Non-Default Users Using the RAMP Heat Template .		
(Optional) Modify the Heat template to configure a GR deployment	Add the parameters AdminSSHKey2 and ssh_authorized_keys.	AdminSSHKey2: type: string label: AdminSSHKey2 description: Access Server public key default: "" ssh_authorized_keys: { get_param: AdminSSHKey2 }	
Cinder volume	A cinder volume must be available. Refer to System Requirements for information on minimum size requirements.	90 GB	Yes

Add Non-Default Users Using the RAMP Heat Template

When you instantiate an instance of Ribbon Application Management Platform (RAMP) on OpenStack, certain user accounts (such as admin) are added by default. You can create additional users through cloud-init by including relevant information in the user_data section of the Heat template.

The following is an example of the section to modify in the Heat template.

```

user_data:
  str_replace:
    template: |
      #cloud-config
      users:
        - name: myadmin
          ssh-authorized-keys:

```

```

- $key1
- $key2
shell: /bin/bash
homedir: /home/myadmin
lock_passwd: false
runcmd:
- sed -i '/^AllowUsers/ s/$/ myadmin/' /etc/ssh/sshd_config
- service sshd restart

```

Admin Password

The RAMP Heat template has an optional parameter, `AdminPassword`, for injecting the password for the admin account. Injecting the admin user password allows console access from any server. (When you instantiate RAMP using the OpenStack Dashboard GUI the corresponding field is **AdminPassword**.)

For more information on how to generate a password, refer to [Generate an Encrypted Password for the RAMP Admin Account](#).

Validate the Downloaded QCOW2 File

Ensure the QCOW2 file you downloaded from the Ribbon Support Portal is intact before using it for installation.

Use this procedure to validate the QCOW2 file.

Start

1. Download the `qcow2.md5` and `qcow2` files to a Linux server.
2. Log on to the Linux server to which the files were downloaded.
3. Enter the following command with the file name:

```
cat <file name>.md5
```

For example:

```
cat ramp-V2x.xx.00R000-RHEL-x.x.xx-x-x86_xx_xx.qcow2.md5
```

A sample output:

```
192b367eb26bfec2bc48f29538c91b47  ramp-V2x.xx.00R000-RHEL-x.x.xx-0-
x86_xx_000.qcow2
```

4. Enter the following command with the file name:

```
md5sum <file name>.qcow2
```

For example:

```
md5sum ramp-V2x.xx.xxRxxx-RHEL-x.x.xx-x-x86_xx_000.qcow2
```

A sample output:

```
192b367eb26bfec2bc48f29538c91b47  ramp-V2x.xx.xxRxxx-RHEL-x.x.xx-x-
x86_xx_xxx.qcow2
```

5. Compare the output from the two commands.
If both values are same, the QCOW2 file is intact.

Create an OpenStack Flavor

Perform the following steps using the OpenStack Dashboard GUI to create an OpenStack flavor for Ribbon Application Management Platform (RAMP) that suits your needs. For information on minimum requirements, refer to [System Requirements](#).

If an OpenStack flavor that matches your configuration requirement already exists, you can reuse an existing flavor. Otherwise, you must be an OpenStack admin user to create an OpenStack flavor.

1. Log on to the OpenStack Dashboard GUI.
2. Click **Admin > Compute > Flavors**. The **Flavors** window opens.
3. Click **Create Flavor**.
4. Add the following details:
 - a. Specify the flavor **Name**.
 - b. By default, the **ID** is auto. You can keep auto, or change it.
 - c. Specify a **vCPUs** value.
 - d. Specify a **RAM (MB)** space.
 - e. Specify a **Root Disk (GB)** space.
 - f. Specify an **Ephemeral Disk (GB)** space of 0 GB.
 - g. Specify a **Swap Disk (MB)** space as 0 MB.
 - h. Specify an **RX/TX Factor** of 1.
5. Click **Create Flavor** to save the flavor with the characteristics you specified..

Enabling CPU Pinning

You have the option to enable CPU pinning on the RAMP flavor.

To enable CPU pinning for RAMP:

1. Log on to the OpenStack CLI as the `admin` user.
2. Enable CPU pinning for the RAMP flavor using the following command:

```
nova flavor-key <flavor-name> set hw:cpu_policy=dedicated
```

The following is an example of enabling CPU pinning for a flavor named "RibbonRAMP."

Example

```
nova flavor-key RibbonRAMP set hw:cpu_policy=dedicated
```

Create a Security Group

Perform the following steps using the OpenStack Dashboard GUI to define security group rules for your Ribbon Application Management Platform (RAMP) deployment. Security group rules define IP traffic rules that allow or deny traffic for the RAMP VM. Add rules that specify the direction to allow (ingress or egress) and the protocol type (TCP, ICMP, UDP).

Ensure that your security group rules enable the features mentioned in [RAMP Security Group Rules](#). If the necessary security group rules are not defined for a feature then it might not work as desired. By default the RAMP template creates security rules for all ports except port 9991.

To add rules:

1. Select **Project > Compute > Access & Security**.
2. The default Security Group defined by the system is displayed. Click **Create Security Group** to define a security group.
3. Provide a name and description for the Security Group. Click **Create Security Group**.
4. Under Actions, click **Manage Rules** for the security group to which you want to add rules.
5. Click **Add Rule** to define a new rule.
6. In the **Add Rule** window, define ingress rules for ICMP traffic and TCP and UDP ports.

Note

The egress rules are defined by default when a security group is created.

7. Click **Add**.
The new rule is listed in the Manage Security Rules screen.

Create an External Network

If an existing external network provides the connection settings you want for your Ribbon Application Management Platform (RAMP) deployment, you can use that existing network. If a suitable network is not already defined, you can define a network using the OpenStack Dashboard GUI.

Note that to create an external network, you must be an OpenStack admin user.

To create an external network using IPv4 addresses, complete the following steps:

1. Click **Admin > Networks**.
2. Click **Create Network** to open the **Create Network** window.
3. Enter a network name, for example ext-net2.
4. In **Project**, select **admin**.
5. In **Provider Network Type**, select **Flat**.
6. In **Physical Network Type** retain default.
7. Ensure **Admin State** is set to **UP**.
8. Check the **Shared** and **External Network** check boxes.
9. Click **Create Network** to create the network and return to the Networks list.
10. Under **Network Name**, click the name of the network to open the **Create Subnet** window and add subnet details.
11. Under **Subnet**:
 - a. Enter a **Subnet Name**.
 - b. Enter the **Network Address** with a prefix (for example: 10.54.28.0/23).
 - c. Select **IPv4** from the **IP Version** list.
 - d. Specify an IP address for the Gateway in the **Gateway IP** field.
 - e. Click **Next**.
12. Under **Subnet Detail**:
 - a. Check **Enable DHCP**.
 - b. Enter an IP pool address range in **Allocation Pools**.
 - c. Add additional **Host Routes**, as necessary.

- d. Click **Create**.

The new network is added to the **Networks** list.

Create a Glance Image

You can create an OpenStack Glance image, using the Ribbon Application Management Platform (RAMP) qcow2 file. You then retrieve the Glance image at the time you launch the RAMP instance.

Use the following procedure to create a Glance image:

1. Log on to the OpenStack Dashboard GUI as an admin user.
2. Click **Project > Compute > Images**. Click **Create Image** on the top-right corner.
3. Provide the following field description in **Create An Image** screen.
 - a. Specify the **RAMP** image name in **Image Name**.
 - b. Enter a description in **Image Description**.
 - c. Click **Browse** and select the qcow2 image file and click **Open**.
 - d. Click **Format** and select **QCOW2 - QEMU Emulator** from the list.
 - e. Under **Image Sharing**, select **Public**.
 - f. Click **Create Image**.

The new Glance image is added to the Images list.

Create a Cinder Volume

Cinder volumes provide persistent storage to VM instances. You must create a cinder volume for the deployment before instantiating an instance. You can use the OpenStack Dashboard to create a cinder volume in a size that fits your deployment's requirements. Refer to [System Requirements](#) for minimum resource requirements.

To create a Cinder volume:

1. Log on to OpenStack Dashboard GUI.
2. Navigate to **Project > Volumes**.
The **Volumes** page opens.
3. In the **Volumes** tab, click **Create Volume**.
The **Create Volume** window opens.
4. Enter a name for the volume in **Volume Name**.
5. Enter a description of the volume in **Description**.
6. Enter the size of the volume in **Size (GiB)**.
7. Click **Create Volume** to create the cinder volume.

Generate an Encrypted Password for the RAMP Admin Account

You need a password in an encrypted format for the admin user account when you instantiate Ribbon Application Management Platform (RAMP).

To generate the password, you can use tools such as mkpassword, openssl, and so on, on a Linux server.

You can use the following procedure to encrypt the password.

Enter the following command:

```
openssl passwd -1 -salt <salt> <password>
```

The following is an example of generating an encrypted version of the password "ribbon"

```
openssl passwd -1 -salt xyz ribbon
```

Sample output:

```
$1$xyz$ZqrM8ZFXx4EzYn0waSuWD/
```

You can use the output as the input value in the **AdminPassword** field in the OpenStack Dashboard GUI when instantiating RAMP.

Generate SSH Keys for RAMP Users

SSH keys for the admin and insight user accounts are required when instantiating Ribbon Application Management Platform (RAMP) on OpenStack.

Generate the SSH keys from a Linux server within the network in order to SSH from that Linux server, as the admin or insight user, without entering the password. You can perform SSH from any other server containing the SSH keys injected during the instantiation.

You can add additional SSH keys after the node instantiation using the `ssh-copy-id` tool. For more information, refer to [Establish Passwordless Connection from an External Server to RAMP](#).

To generate SSH keys:

1. Verify that the files `id_rsa` and `id_rsa.pub` exist on a Linux server and then enter the following command on the server:

```
ssh-keygen
```

The following message is displayed:

```
Generating public/private rsa key pair.
Enter file in which to save the key (<the home directory of the Linux
server>/.ssh/id_rsa):
```

2. Press **ENTER**:
The following message is displayed:

```
<the home directory of the Linux server>/.ssh/id_rsa already exists.
Overwrite (y/n)?
```

3. Enter **y**.
The following prompt is displayed:

```
Enter passphrase (empty for no passphrase):
```

4. Press **Enter**.
The following prompt is displayed:

```
Enter same passphrase again:
```

Example output:

```

Your identification has been saved in <the home directory of the Linux
server>/.ssh/id_rsa.
Your public key has been saved in <the home directory of the Linux server>/.ssh/
id_rsa.pub.
The key fingerprint is:
SHA256:NqYFcc0h0Jurdk6hBSQU+BCyV/UQwJBqNt3UUnQRf+I insight@treebeardVm3
The key's randomart image is:
+---[RSA 2048]-----+
| . oB*+@*o*+ . |
| o+..= *o.+ |
| ..ooo + .o o . |
| .= ... oo . o |
| o . S. E |
| B.o |
| o.. |
| o.. |
| . o. |
+-----[SHA256]-----+

```

Use the text in the file `<the home directory of the Linux server>/.ssh/id_rsa.pub` as input value in the following fields in OpenStack Dashboard GUI when you instantiate RAMP:

- AdminSSHKey
- InsightSSHKey

After you initiate RAMP using `id_rsa.pub`, you can log on using the SSH keys. For more information, refer to [SSH to RAMP using SSH Keys](#).

SSH to RAMP using SSH Keys

To create the Ribbon Application Management Platform (RAMP) on OpenStack, use the SSH keys for the admin and insight user accounts.

Perform the following steps to log on to the RAMP:

```
ssh -i id_rsa admin@<RAMP IP>
```

Sample output

```

bats12:~/VNFMKey> ssh -i id
id_rsa      id_rsa.pub
bats12:~/VNFMKey> ssh -i id_rsa admin@10.34.146.32
The authenticity of host '10.34.146.32 (10.34.146.32)' can't be established.
ECDSA key fingerprint is SHA256:s4H3wPQbQ3W8hAbJI4VxTjGURKJQrZB85wU6j1px6Dw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.34.146.32' (ECDSA) to the list of known hosts.
*****

```

```

** The RAMP Successfully Started          **
*****
** Version info use this command:      **
** rpm -q SONSems                        **
*****
** This file is called /etc/motd         **
*****
Last login: Fri Feb 23 16:46:51 2024 from 10.54.81.11
OS      : Red Hat Enterprise Linux 8.9 (Ootpa)
Kernel  : 4.18.0-513.11.1.el8_9.x86_64
Ribbon  : 8.9.85-136

[2024-02-23 16:46:52 admin@cicdDmRestmicroEMS: ~ ]#

```

Copy SSH Keys to Instantiate a RAMP Standby Instance

To copy SSH keys to the Ribbon Application Management Platform (RAMP) standby instance in a geo-redundant (GR) deployment:

1. Access the RAMP active instance as the admin user.
2. Copy the ssh key from this directory:

```
cat /home/admin/.ssh/id_rsa.pub
```

3. Use the contents of the file as input value for the following fields in the OpenStack Dashboard GUI when instantiating the standby instance:
 - AdminSSHKey
 - AdminSSHKey2

Enter the AdminSSHKey2 from the active RAMP to establish passwordless connection between the active and standby nodes.

- InsightSSHKey

Instantiate RAMP on OpenStack

The following procedure describes how to launch a Ribbon Application Management Platform (RAMP) instance using the OpenStack Dashboard GUI. Before you begin, complete the steps to prepare your environment for instantiation outlined in the Installation workflow table on [Installing RAMP on OpenStack](#).

Review the table below that describes the parameters present in the RAMP template. Enter or edit the parameters to launch the instance. In particular, prepare to enter the following instantiation details:

- Management Fixed address/Prefix
- Lawful Intercept Fixed address/Prefix
- Management Gateway address
- Lawful Intercept Gateway address

Before instantiating the RAMP, populate an environment file with the respective IP addresses for your environment. While launching a stack with the template files, specify the environment file name, which directly populates the parameters with the specified values.

Select both the Heat template and the environment file from the **Select Template** window when using the environment file. Alternatively, you can launch using the Heat Template and then update the parameter values during instantiation.

Note

Use the `RAMP_HEAT_TEMPLATE_SEC_MGMT.yaml` to include the secondary interface (MGT1). This template is part of the `templates.tar` file.

Where LI is replaced with the secondary interface (MGT1) in the template parameters, LI is not supported if the `RAMP_HEAT_TEMPLATE_SEC_MGMT.yaml` is used.

To instantiate the RAMP standalone instance:

Start

1. Log on to the **OpenStack** GUI as an `admin` user.
2. On the navigation pane, click **Orchestration > Stacks**.
3. In the top-right corner, click **Launch Stack**.
The **Select Template** window displays.
4. Click **Browse** under **Template File** and select the Heat template file.
5. (Optional) Click **Browse** under **Environment File** and select an environment file to use to populate values when you launch the Stack.
6. Click **Next**.
7. In the **Launch Stack** window, enter the values as specified in the following Parameters table:

Note

To access the RAMP GUI, select 1 to use in the Floating IP count and 0 to not use the **Floating IP count** in your network. Specify only the **External Network Id** and **LI External Network Id** values, if the **Floating IP count** is set to 1.

Parameters

Field	Description	Example Values
Stack Name	A unique name for the stack.	RAMPSA
Creation Timeout (minutes)	Time in minutes for stack creation time-out. The default value is 60 minutes.	60

Field	Description	Example Values
Rollback on Failure	If you do not want to view any stack creation log or update, select the Rollback on Failure checkbox.	
OpenStack user password	User password to log into the OpenStack Dashboard which is required to perform operations throughout the stack lifecycle.	admin
AdminPassword	The encrypted password generated for the RAMP admin user. To generate an admin password, refer to Generate an Encrypted Password for the RAMP Admin Account .	
AdminSSHKey	SSH key generated on a Linux server. To generate the SSH key, refer to Generate SSH Keys for RAMP Users .	
AdminSSHKey2	The SSH key of the admin user in the active RAMP to establish a passwordless connection between the active and standby nodes. Note The parameter is applicable only for GR. Refer to Checklist for Installing RAMP on OpenStack. SSH key generated on a Linux server. To generate SSH key, refer to Generate SSH Keys for RAMP Users	
Dns Servers	(Optional) If you have a DNS server, specify the DNS server IP address. Note: If you have multiple DNS servers, then it can be specified as [fd00:10:6b50:4500::3, fd00:10:6b50:4500::4].	fd00:10:6b50:4500::3
External Network Id	Only required if you set Floating IP Count to 1.	
LI External Network Id	Only required if you set Floating IP Count to 1.	

Field	Description	Example Values
Flavor	Select the RAMP flavor, you want to apply to the Stack.	RAMP_Flavor
Floating IP count	Set to 1 to assign a separate floating IP address to access the RAMP GUI. Set to 0 if you do not want to use a floating IP address to access the RAMP GUI.	To use a floating IP address, select 1
IP Version v4/v6	Depending on the IP address type configured in the network, select V4 for IPv4 and V6 for IPv6. Ensure you configure other network IP address parameters for the selected type.	
Image	The unique name of the OpenStack Glance image created using the RAMP qcow2 image file.	RAMP_22.06.R000
InsightSSHKey	SSH key generated on a Linux server. To generate the SSH key, refer to Generate SSH Keys for RAMP Users .	
LI Mediation Server port	This port number is automatically filled in.	
Management Fixed IP	Specify the fixed management IP address from the available range of provider network management IP addresses. Note If the IPv6 address contains 7 octets, enter at least one digit for the all-zero group to make it 8 octets. Incorrect: 2607:f160:b:105a:cf:209::20 Correct: 2607:f160:b:105a:cf:209:0:20	fd00:10:6b50:43a0::a1

Field	Description	Example Values
LI Management Fixed IP	Specify the LI fixed management IP address from the available range of LI management IP addresses. Note If the IPv6 address contains 7 octets, enter at least one digit for the all-zero group to make it 8 octets.	fd00:10:6b50:4360::c9
Management Fixed IP Prefix	Specify the prefix for IPv4 or IPv6 configured in your management network.	60
LI Management Fixed IP Prefix	Specify the prefix for IPv4 or IPv6 configured in your LI management network.	60
Management Gateway IP	Specify the management gateway IP address.	fd00:10:6b50:43a0::1
LI Management Gateway IP	Specify the LI management gateway IP address.	fd00:10:6b50:4360::1
Management Network Id	Specify the management network ID for the provider management network.	955ccb6b-dbc4-44d5-bc8e-3084d0e739c6
LI Network Id	Specify the LI management network ID configured in your network.	provider-pkt0
Management Network Port Name	Specify the management network port name for the provider management network.	mgmt-pr-v4
Management Subnet Id	Specify the management subnet ID for the provider management network.	5ea0abf6-7bc1-46f6-8392-e7e11cd0fa83
LI Management Subnet Id	The LI management subnet ID configured in your network.	5369f101-059b-4d61-9520-32df6c3581a2

Field	Description	Example Values
Ntp Servers	(Optional) Specify the NTP server IP address if you have an NTP server. To add multiple NTP servers, enter the IP addresses in the following format: <pre><NTP server 1>,<NTP server 2>,<NTP server 3></pre> Example: <pre>10.1.1.6,10.128.254.67,10.128.254.68</pre>	fd00:10:6b50:4500::11
TimeZone	Specify the time zone for your network.	America/Chicago
Volume Id	Specify the ID of the Cinder volume to associate with the RAMP instance.	4db35a5b-849d-4c88-a9a0-7f2c31b8652d

8. (Optional) If your internal network is clashing with the networks created by the docker service, then add a file named `/opt/rbbn/dockerNetworksFile` through the user-data or the HEAT template. This file validates and writes the data to the `/etc/docker/daemon.json` file. For more information on Docker Daemon, refer to [RAMP Customization for Docker Daemon](#).

Note

You must add a minimum of seven networks for the RAMP 24.06 release. You are allowed to add networks that suit you but do not change the variable names.

IPv6 support is currently disabled.

Example code

```
write_files:
  - path: /opt/rbbn/dockerNetworksFile
    permissions: '0744'
    owner: root:root
    content: |
      dockerNetwork1=172.21.0.0/16
      dockerNetworkSize1=24
      dockerNetwork2=172.22.0.0/16
      dockerNetworkSize2=24
      dockerNetwork3=172.23.0.0/16
      dockerNetworkSize3=24
```

```

dockerNetwork4=172.24.0.0/16
dockerNetworkSize4=24
dockerNetwork5=172.25.0.0/16
dockerNetworkSize5=24
dockerNetwork6=172.26.0.0/16
dockerNetworkSize6=24
dockerNetwork7=172.27.0.0/16
dockerNetworkSize7=24

```

9. Click **Launch**.
A "Stack creation in progress message" appears.
Once the stack is created, the status changes to **Create Complete**.
10. Complete the remaining steps to verify the instantiation.
11. Click on **Stack Name** and verify that the Topology is up.
12. From the navigation pane:
 - a. click **Project > Compute > Access & Security**. Verify that security groups were created during RAMP instantiation,
 - b. click **Project > Compute > Cinder Volume**. Verify that the Cinder volume was attached to the RAMP instance, and

Note

The LI interface is also created as part of the RAMP instantiation.

Once the LI Interface is created, you can configure a distributed SBC for Lawful Interception.

- c. click **Project > Compute > Instances**. Verify that the RAMP standalone instance is active and running.
13. Wait approximately 15 minutes for the GUI to become accessible and then log onto the RAMP GUI as an admin user. Use the floating IP address if you configured one. Otherwise, use the RAMP fixed IP address.

Instantiating and Managing RAMP using VNFM

Additional sections:

- [Installing Standalone RAMP using VNFM](#)
 - [Pre-Instantiation Checklist for RAMP Standalone using VNFM](#)
 - [Create an OpenStack Flavor using Dashboard for VNFM](#)
 - [Create a Glance Image using Dashboard for RAMP Instantiation Using VNFM](#)
 - [Define a Network Configuration using Dashboard for RAMP Instantiation Using VNFM](#)
 - [Create a New Tenant in the OpenStack Dashboard IP](#)
 - [Create a New User in the OpenStack Dashboard IP](#)
 - [Add a Cloud from the UI](#)
 - [SSH Keys for RAMP Users to Instantiate using VNFM](#)
 - [Configure a Tenant](#)
 - [Onboard VNFs Using CSAR Packages](#)
 - [Instantiate a VNF](#)

Ribbon VNFM supports instantiating and managing the Ribbon Application Management Platform (RAMP) VNF instances, including interfacing with network orchestrators (NFVO) by using a `yaml` file (`ramp-vnfd.yaml`) combined in a Cloud Service Archive (CSAR) file to deploy RAMP VNF instances.

RAMP VNF instantiation using VNFM is supported on Newton and later versions of OpenStack release.

Ve-VNFM communication uses the management interface for all the VNFs.

Note

RAMP does not support VNFR. Due to this in VNFM RAMP remains in an Orchestrated state. Only RAMP install and terminate operations are supported from VNFM.

Instantiation is supported using the CSAR package for RAMP and RAMP GEO with virtio network and static IP assignment.

RAMP deployment variations using same CSAR package	IP addressing support
RAMP Active/Source (1 mgmt, 1 config) using provider networks	IPv4 and IPv6 with static addressing
RAMP GR/Target (1 mgmt, 1 config) using provider networks	IPv4 and IPv6 with static addressing

The RAMP Active and Geo-redundancy (GR) VMs are deployed as standalone systems. The RAMP standalone system is deployed in 1+0 mode and does not require anti-affinity.

You can instantiate RAMP active or source or GR VNFs that enable VM to:

- Mount cinder volume for persistent data store (Configuration and OAMs) and ephemeral for root disk.
- Configure Management and Configuration (LI) interfaces.

RAMP VNFs includes the following VNIC definitions in the CSAR VNFD:

- VNIC Types
 - Management Interface - IPV4/IPV6, Static, virtio type.
 - LI Configuration interface - IPV4/IPV6 Static, virtio type.
- VNIC Redundancy provided by platform OVS and Virtual Connect switching layers.
- Traffic is normally untagged. If applicable, tagged traffic is validated.

You can add security groups for the RAMP VM on VM level in the CSAR VNFD and orchestrate the VM, as well as validate the traffic against the security group configuration.

Installing Standalone RAMP using VNFM

Additional sections:

- [Pre-Instantiation Checklist for RAMP Standalone using VNFM](#)
- [Create an OpenStack Flavor using Dashboard for VNFM](#)
- [Create a Glance Image using Dashboard for RAMP Instantiation Using VNFM](#)
- [Define a Network Configuration using Dashboard for RAMP Instantiation Using VNFM](#)
- [Create a New Tenant in the OpenStack Dashboard IP](#)
- [Create a New User in the OpenStack Dashboard IP](#)

- [Add a Cloud from the UI](#)
- [SSH Keys for RAMP Users to Instantiate using VNFM](#)
- [Configure a Tenant](#)
- [Onboard VNFs Using CSAR Packages](#)
- [Instantiate a VNF](#)

Perform the following steps to instantiate VNFM on the Ribbon Application Management Platform (RAMP).

The workflow below provides an overview of the process and provides links to the specific information and steps required to complete installation. After completing the steps on a linked page, return to the workflow for the next procedure.

Step	Action	Link to Procedure
1	Review the pre-instantiation checklist.	Pre-Instantiation Checklist for RAMP Standalone using VNFM
2	Create an OpenStack Flavor with specified RAM, Disk size, and CPU details.	Create an OpenStack Flavor using Dashboard for VNFM Note NOTE: If you already have an OpenStack Flavor with the appropriate configuration, you can reuse the existing OpenStack Flavor. Refer to System Requirements.
3	Define management external network.	Define a Network Configuration using Dashboard for RAMP Instantiation Using VNFM
4	Create a new tenant in the OpenStack Dashboard IP.	Create a New Tenant in the OpenStack Dashboard IP
5	Create a new user in the OpenStack Dashboard IP.	Create a New User in the OpenStack Dashboard IP
6	Add the OpenStack Dashboard IP to VNFM.	Add a Cloud from the UI
7	Add the OpenStack tenant to VNFM.	Configure a Tenant
8	Create a RAMP image on the Glance image server.	Create a Glance Image using Dashboard for RAMP Instantiation Using VNFM
9	Generate admin password in encrypted format.	Generate an Encrypted Password for the RAMP Admin Account

Step	Action	Link to Procedure
10	Generate SSH keys.	Generate SSH key to Instantiate a Standalone RAMP using VNFM
11	Onboard VNF on VNFM.	Onboard VNFs Using CSAR Packages
12	Onboard VNF on VNFM.	Instantiate a VNF
13	Note This step is applicable only for GR. Configure RAMP Geographical Redundancy (GR).	Configuring RAMP Redundancy
14	Perform post-instantiation tasks.	Post-RAMP Instantiation Tasks

Pre-Instantiation Checklist for RAMP Standalone using VNFM

This section provides information on how to set up the required environment before launching an instance of the Ribbon Application Management Platform (RAMP). The environment set up is a one-time activity, once the environment is set up, one or several RAMP instances can be launched.

The checklist consists of a list of planning information you should complete before you start instantiating RAMP using VNFM. You can tick each task as you complete it and make notes in the **Comments** column below. Ribbon recommends that you make note of the parameter values that you need to enter during the instantiation process and while configuring RAMP.

Parameter	Description	Example	Mandatory?	Comments
OpenStack GUI Dashboard Prerequisites:				
OpenStack Dashboard GUI URL	To access OpenStack dashboard on the controller, type the URL in browser.	<pre>http:// <controller-IP>/ dashboard</pre> Replace the <controller-IP> with your IP address, for example: <pre>http://10.54.27.112/ dashboard/</pre>	Yes	

Parameter	Description	Example	Mandatory?	Comments
OpenStack Dashboard GUI Login credentials	The username and password to access the OpenStack GUI dashboard.	username: admin password: admin	Yes	
OpenStack CLI Prerequisites:				
Setting Environment variables in <code>admin-openrc.sh</code> environment file.	Create an environment file <code>admin-openrc.sh</code> and set the environment variables with desired values for OpenStack command-line client access. The mandatory environment variables to be configured are: <code>OS_USERNAME</code> <code>OS_PASSWORD</code> <code>OS_TENANT_NAME</code> <code>OS_AUTH_URL</code>	Example values for environment variables are: <code>OS_USERNAME=admin</code> <code>OS_PASSWORD=admin</code> <code>OS_TENANT_NAME=admin</code> <code>OS_AUTH_URL=http://10.54.27.112:35357/v2.0</code> Replace the above values as per your requirements.	Yes	
Source the environment file	Note: Before executing any CLI command in a new console session, ensure that you set the environment variables using <code>source admin-openrc.sh</code> script. To set the environment variable changes to effect and allow execution of OpenStack CLI, you must source the <code>admin-openrc.sh</code> file.	Example: <code>source admin-openrc.sh</code>	Yes	
Common Prerequisites:				
External Network (ext-net)	The external routable IP address given by the lab-team.	10.9.9.97	Yes	

Parameter	Description	Example	Mandatory?	Comments
Download RAMP qcow2 image from the RAMP software bundle available in the Support Portal. For more information, refer to Download Files from Ribbon Support Portal .	The RAMP qcow2 image package for OpenStack.	<i>ramp-V24.03.00R000-RHEL-07.xx.xx.xx-x86_64_80.qcow2</i>	Yes	
Download the CSAR image from the RAMP software bundle available in the Support Portal. For more information, refer to Download Files from Ribbon Support Portal .	The CSAR files to instantiate RAMP SA and GR instances.	<i>ramp-Vxx.xx.00xxxx-xxxx-xxxx.tar.gz</i>	Yes	

Create an OpenStack Flavor using Dashboard for VNFM

Create an OpenStack flavor of the Ribbon Application Management Platform (RAMP) on the VNFM.

Create OpenStack Flavor

Perform the following procedure to create an OpenStack flavor. You can reuse an existing OpenStack flavor if it matches your configuration requirements. Create an OpenStack flavor that suits your needs using the Dashboard GUI. For requirements details, refer to [System Requirements](#).

Note

The admin user creates flavors on OpenStack. If you are a non-admin user, consult your admin user to create a flavor.

Note

The following example demonstrates creating a RAMP flavor for large configurations.

Start

1. To create a flavor, logon to the OpenStack GUI dashboard.
2. Navigate to **Admin > Flavors**.
The **Flavors** window is displayed.
3. Click **Create Flavor** to define a new flavor.
4. Add the following details to create a flavor:
 - a. Specify the flavor name.
 - b. By default, the ID is auto. You can keep it auto or change it.

- c. Enter **vCPU** value as 16.
- d. Enter **RAM (MB)** space as 65336.
- e. Enter **Root Disk (GB)** space as 90 GB.
- f. Enter **Ephemeral Disk (GB)** space as 0 GB.
- g. Enter **Swap Disk (MB)** space as 0 MB.
- h. Enter **RX/TX Factor** as 1.
- i. Click **Create Flavor** to save the flavor.

Enable CPU Pinning

Use this procedure to enable CPU Pinning after creating the RAMP flavor.

Note

CPU Pinning is optional for RAMP.

Start

1. Logon to OpenStack CLI as the `admin` user.
2. Enable RAMP CPU Pinning:

```
nova flavor-key <flavour-name> set hw:cpu_policy=dedicated
```

The following is an example of enabling RAMP CPU Pinning with the flavor-name of "SONUSRAMP."

```
nova flavor-key SONUSRAMP set hw:cpu_policy=dedicated
```

Create a Glance Image using Dashboard for RAMP Instantiation Using VNFM

A glance image enables discovering, registering, and retrieving virtual machine images. Create a glance image of a container with the application qcow2 image that you will use when creating a small or large VM flavor. This image provides the preinstalled application when you launch the instance.

Perform the following procedure to create a glance image:

1. Log on to the OpenStack GUI as admin user.
2. Navigate to **Project > Images**. Click **+Create Image** on the top-right corner.
3. Provide the following field description in **Create An Image** screen.
 - a. Specify the RAMP Image name in **Name** field.
 - b. Enter a relevant description in **Image Description** field.
 - c. Click **Browse** and select the qcow2 image file and click **Open**.
 - d. Click **Format** and select **QCOW2 - QEMU Emulator** from the drop-down menu.
 - e. Select the check-box **Public**.
 - f. Click **Create Image**.

The glance image is created and displayed.

Define a Network Configuration using Dashboard for RAMP Instantiation Using VNFM

Use this section to create an external network with the desired IPv4 addresses.

Note

If existing external networks are already defined with the desired connection settings, you can use the existing available networks. If networks are not defined, use the following procedure to define your networks.

Create External Network

Start

1. Click **Admin > Networks**. RAMP displays the **Networks** window.
2. Click **Create Network** to define the networks.
3. Create an external network:
 - a. Type the network name for example **ext-net2**.
 - b. Select the **Project** as **admin**.
 - c. Select **Provider Network Type** as **Flat**.
 - d. Retain the **Provider Network Type** as default.
 - e. Ensure **Admin State** is UP.
 - f. Select the **Shared** and **External Network** check boxes.
 - g. Click **Create Network**.
4. Click **ext-net2** link from Network Name and add the subnet details.
5. In **Subnet** tab, set the subnet:
 - a. Specify the Subnet Name.
 - b. Enter the network address with prefix (for example: 10.54.28.0/23).
 - c. Select the IPv4/v6 version from pull-down list.
 - d. Enter the Gateway IP address (normally use the first value of the IP address range) .
 - e. Click **Next**.
6. In the **Subnet Detail** tab,
 - a. Specify the IP pool address range in Allocation Pools.
 - b. Add any additional host routes as necessary.
 - c. Click **Create**.

Create a New Tenant in the OpenStack Dashboard IP

Perform the following procedure to create a new tenant for the Ribbon Application Management Platform (RAMP) VNF on OpenStack:

Start

1. Log on to OpenStack GUI.
2. Navigate to **Identity > Projects**.
3. Click **Create Project**.

Create a New User in the OpenStack Dashboard IP

Perform the following procedure to create a new user (non-admin) for the Ribbon Application Management Platform (RAMP) VNF on OpenStack:

Start

1. Log on to the OpenStack GUI.
2. Navigate to **Identity > users**.
3. Click **Create User**. The **Create User** dialog box is displayed.

Note

Set the role as **heat_stack_user**.

4. Click **Create User**.

Add a Cloud from the UI

Use the following procedure to target each Cloud you add to the VNFM to a specific VNF deployment.

Adding a Cloud

Use the following procedure to add a VIM through the UI.

1. Log into the VNFM UI. See [Logging into the VNFM UI](#).
2. Select **VNFM Configuration>Clouds**.

List of configured clouds

Cloud Name	Identity (Keystone)	Compute (Nova)	Networking (Neutron)	Image (Glance)	Block Storage (Cinder)	Actions
Ottawa_PC2	172.29.49.201:5000 (v3)	172.29.49.202:8774 (v2.1)	172.29.49.207:9696 (v2.0)	172.29.49.203:9292 (v2.6)	172.29.49.204:8776 (v3)	

3. Click **Add Cloud** in the Clouds panel to open the Add Cloud window.

Add Cloud - no version numbers on left, used Get Version button on right

Clouds > Add Cloud

Add Cloud

Cloud Config

Cloud Name

SVT_Cloud

Identity (Keystone) API Endpoint IP Address

svtcloud2.eng.sonusnet.com

13000

Version

Compute (Nova) API Endpoint IP Address

svtcloud2.eng.sonusnet.com

13774

Version

Networking (Neutron) API Endpoint IP Address

svtcloud2.eng.sonusnet.com

13696

Version

Block Storage (Cinder) API Endpoint IP Address

svtcloud2.eng.sonusnet.com

13776

Version

Image (Glance) API Endpoint IP Address

svtcloud2.eng.sonusnet.com

13292

Version

API Endpoint Protocol

HTTPS

Get Version

Cancel

Save

Clouds > Add Cloud

Add Cloud

Cloud Config

Cloud Name
SVT_Cloud

Identity (Keystone) API Endpoint IP Address
svtcloud2.eng.sonusnet.com
13000
v3

Compute (Nova) API Endpoint IP Address
svtcloud2.eng.sonusnet.com
13774
v2.1

Networking (Neutron) API Endpoint IP Address
svtcloud2.eng.sonusnet.com
13696
v2.0

Block Storage (Cinder) API Endpoint IP Address
svtcloud2.eng.sonusnet.com
13776
v3

Image (Glance) API Endpoint IP Address
svtcloud2.eng.sonusnet.com
13292
v2.4

API Endpoint Protocol
HTTPS

✓ **Success:** Keystone (v3: stable, v2.0: deprecated) Nova (v2: supported, v2.1: current) Block Storage (v1: deprecated, v2: supported, v3: current) Image (v2.4: current, v2.3: supported, v2.2: supported, v2.1: supported, v2.0: supported, v1.1: deprecated, v1.0: deprecated) Neutron (v2.0: current)

Get Version
Cancel
Save

In the Cloud Config section,

- Create a name to identify the target VIM in the Cloud Instance Name field. The name cannot contain square brackets ([]). The chosen name is used by the VNFM to identify the cloud on the UI and in logs. There is no external dependency on the value.
- Select the API Endpoint Protocol (HTTP or HTTPS) using the drop-down.
- Enter the API endpoints for the VIM in the Identity, Compute, Networking, Block Storage (optional), and Image API Endpoint IP Address fields. If any of the service IPs are entered, the **Get Version** button is enabled, however be sure to populate all the service IPs to retrieve the versions for each one. When you click the **Get Version** button, VNFM queries OpenStack to retrieve the current, stable, supported, and deprecated versions for the service. The version drop-down is populated with these values. The default value of the drop-down is set to either the current, stable, supported, or deprecated version, in that order, depending on the values returned.

Note

When entering IPv6 addresses, square brackets ([]) must be entered around each IPv6 address. For example: [fd00:0:a23:1239::77].

Note

The version number of the Openstack services is dependent on deployment. Ensure the version values and format are accurate for the specified address. Incorrect version numbers and version formats, such as v2 versus v2.0, prevent the deployment of a VNF.

In the example above, the Add Cloud window on the left shows IP addresses entered without version numbers. The example Add Cloud window on the right shows the results of selecting the **Get Version** button. Clicking the **Get Version** populates the version fields and indicates which other versions are available from the specified cloud. If your VNFM VMs support DNS (Heat templates have been updated to support a list of DNS entries), and are configured to support Fully Qualified Domain Name (FQDN), then FQDN entries are allowed in the IP address fields when configuring a cloud.

Notes

Enter the VIM endpoint in the <IP_Address> field as an IP address or FQDN if DNS is configured. Enter the port number in the separate <port_number> field.

Default ports are assumed; however, non-default port numbers can be explicitly provided in the port number field. Non-default ports may need to be added to security group rules and may not be compatible with Load Balancer proxy settings.

4. Click **Save**.
5. A successful configuration of the target Cloud instance sends a notification and creates an entry in the Cloud panel on the **VNFM Configuration>Clouds** screen.

SSH Keys for RAMP Users to Instantiate using VNFM

When you instantiate the Ribbon Application Management Platform (RAMP) using VNFM, the 'admin' and 'insight' user SSH keys are injected into the RAMP using the **Cloud Config Init Data**. At this point, all scripts use passwordless-SSH and password-prompted SSH.

- InsightSSHKey
- AdminSSHKey

To generate or copy or SSH keys, refer to:

- [Generate SSH key to Instantiate a Standalone RAMP using VNFM](#)
- [Copy SSH key to Instantiate the Target RAMP Instance using VNFM](#)

Generate SSH key to Instantiate a Standalone RAMP using VNFM

An SSH key pair is required to instantiate the Ribbon Application Management Platform (RAMP) using VNFM.

Perform the following procedure to generate the SSH keys:

Start

1. Run the following command on a Linux server:

Note

Check if the files `id_rsa` and `id_rsa.pub` exist on the Linux server.

```
ssh-keygen
```

The following prompt displays:

```
Generating public/private rsa key pair.
Enter file in which to save the key ($USER_HOME_DIR/.ssh/id_rsa):
```

2. Press **ENTER**. The following prompt displays:

```
$USER_HOME_DIR/.ssh/id_rsa already exists.
Overwrite (y/n)?
```

3. Enter "y". The following prompt displays:

```
Enter passphrase (empty for no passphrase):
```

4. Press **Enter**. The following prompt displays:

```
Enter same passphrase again:
```

The following output displays:

```
Your identification has been saved in $USER_HOME_DIR/.ssh/id_rsa.
Your public key has been saved in $USER_HOME_DIR/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:NqYFcc0h0Jurdk6hBSQU+BCyV/UQwJBqNt3UUnQRf+I insight@treebeardVm3
The key's randomart image is:
+---[RSA 2048]-----+
| . oB*+@*o*+. |
| o+..= *o.+ |
| ..ooo + .o o . |
| .= ... oo . o |
| o . S. E |
| B.o |
| o.. |
| o.. |
| . o. |
+-----[SHA256]-----+
```

5. Use the text in the file `$USER_HOME_DIR/.ssh/id_rsa.pub` (depending on the user) as input value for the **Cloud Config Init Data** field:


```

runcmd:
- usermod -p '<encrypted admin password>/' admin
users:
- name: insight
ssh_authorized_keys:
- <SSH key>
- name: admin
ssh_authorized_keys:
- <SSH key>

```

For example:

```

runcmd:
- usermod -p '$6$BzdlFaNVC.etRjAZ$IDW8ytHjH2AlSNGwu5/dnnLTV.gjbpTyMbSYguA.g.U1iOy9Bm3sKb8TKADo4UnFfzsqFwr67fNEfhnJVxTt0.' admin

users:
- name: insight
  ssh_authorized_keys:
    - ssh-rsa
    AAAAB3NzaC1yc2EAAAABIwAAAIEAvf4xCxJ7KCuskBsEeMtHEreEfv0n6Rc7SG6chSayooWl6q4RIRAPgV
    Ym7UciMwxZy7bseQ1DJE2WkumA7kU0myvzsMfkXemXK63Uc7PWZMt2htHWAqn2As1ZfKchzprXWc2zGX7C
    fMELckr36SztTjcQMzX+atyCp00L+uwNs= jklotzbach@insight
- name: admin
  lock_passwd: false
  ssh_authorized_keys:
    - ssh-rsa
    AAAAB3NzaC1yc2EAAAABIwAAAIEAvf4xCxJ7KCuskBsEeMtHEreEfv0n6Rc7SG6chSayooWl6q4RIRAPgV
    Ym7UciMwxZy7bseQ1DJE2WkumA7kU0myvzsMfkXemXK63Uc7PWZMt2htHWAqn2As1ZfKchzprXWc2zGX7C
    fMELckr36SztTjcQMzX+atyCp00L+uwNs= jklotzbach@insight
    AAAAB3NzaC1yc2EAAAABIwAAAIEAvf4xCxJ7KCuskBsEeMtHEreEfv0n6Rc7SG6chSayooWl6q4RIRAPgV
    Ym7UciMwxZy7bseQ1DJE2WkumA7kU0myvzsMfkXemXK63Uc7PWZMt2htHWAqn2As1ZfKchzprXWc2zGX7C
    fMELckr36SztTjcQMzX+atyCp00L+uwNs= jklotzbach@insight

```

Copy SSH key to Instantiate the Target RAMP Instance using VNFM

Use this procedure to copy the SSH key to instantiate a target Ribbon Application Management Platform (RAMP) instance using VNFM. For the GR target, pass the SSH keys from the RAMP source instance.

Start

To copy the "insight" SSH keys for the RAMP GR:

1. On the source RAMP, ssh as admin user:

```
ssh admin@<EMS source instance IP>
```

The following is an example:

```
ssh admin@10.54.58.172
```

2. Change to `root` user:

```
su - root
```

3. Enter the `root` password.

```
Password:
```

4. Change to `insight` user:

```
su - insight
```

5. Copy the `ssh` key for the insight user from the following path:

```
/opt/sonus/ems/.ssh/id_rsa.pub
```

6. Use the text in the file `/opt/sonus/ems/.ssh/id_rsa` (depending on the user) as input value for the **Cloud Config Init Data** field:

```
runcmd:
- usermod -p '<encrypted admin password>/' admin
users:
- name: insight
ssh_authorized_keys:
- <SSH key>
- name: admin
ssh_authorized_keys:
- <SSH key>
```

For example:

```
runcmd:
- usermod -p '$6$BzdlFaNVC.etRjAZ$IDW8ytHjH2A1SNGwu5/dnnLTV.gjbpTyMbSYguA.g.U1iOy9Bm3sKb8TKADo4UnFfzsqFwr67fNEfhnJVxTt0.' admin

users:
- name: insight
  ssh_authorized_keys:
    - ssh-rsa
    AAAAB3NzaC1yc2EAAAABIwAAAIEAvf4xCxJ7KCuskBsEeMtHEreEfv0n6Rc7SG6chSayooWl6q4RIRAPgV
    Ym7UciMwxZy7bseQ1DJE2WkumA7kU0myvzsMfkXemXK63Uc7PWZMt2htHWAqn2As1ZfKchzprXWc2zGX7C
    fMELckr36SzqTjcQMzX+atyCpPP00L+uwNs= jklotzbach@insight
```

```
- name: admin
  lock_passwd: false
  ssh_authorized_keys:
    - ssh-rsa
    AAAAB3NzaC1yc2EAAAABIwAAAIEAvf4xCxJ7KCuskBsEeMtHEreEfv0n6Rc7SG6chSayooWl6q4RIRAPgV
    Ym7UciMwxZy7bseQ1DJE2WkumA7kU0myvzsmFkXemXK63Uc7PWZMt2htHWAqn2As1ZFkchzprXWc2zGX7C
    fMELckr36SzqTjcQMzX+atyCp00L+uwNs= jklotzbach@insight
```

Configure a Tenant

In this section:

- [Configuring VNF tenants - Overview](#)
 - [Adding VNF Tenant Accounts](#)
 - [Editing VNF Tenant Accounts](#)
 - [Deleting a VNF Tenant Account](#)

Configuring VNF tenants - Overview

Tenants which are referred to in OpenStack as projects, may support multiple VNF instances. An authorized user can add, edit, or delete tenant accounts through the UI providing sufficient resources are available to support the tenants.

Adding VNF Tenant Accounts

Use the following procedure to configure the VNF tenant account. Each tenant can host multiple VNF deployments.

1. Log into the VNFM UI. See [Logging into the VNFM UI](#).
2. Select **VNFM Configuration>Tenants**.
3. In the Tenants panel, click **Add Tenant**.
4. In the **Add Tenant** panel,
 - a. Enter the OpenStack VIM tenant name in the cloud *Tenant Name* field. This name must match the OpenStack project name and cannot contain square brackets ([]).

Note

Be careful when copying the name from an OpenStack project name to not include the space character.

- b. Enter a domain for the associated cloud in the *Domain* field. This name must match a domain from the OpenStack VIM in which the tenant is hosted. The default value is "Default". If the *Domain* field is empty "Default" is configured. The Domain field syntax contains a user domain and a project domain separated by a "/" (<user domain> (optional) / <project domain>). The project domain is optional. This means if default is chosen, the Domain field entry is Default (using only the user domain) or Default/Default (using Default both the user and project domain).
 - c. Enter a user name for the associated cloud in the *Cloud User Name* field. This name must match a user name from the OpenStack VIM in which the tenant is hosted, with permission to access that tenant.
 - d. Enter a password for the associated cloud in the *User Password* field. This name must be the password associated with the Cloud User Name.

- e. Select the associated cloud from the *Associated Cloud* drop-down. This maps the project to its associated VIM instance.

Add Tenant Panel

Tenants > Add Tenant

Add Tenant

Tenant Usage

Live VNF Status: Totals

Instance Count (VNFs)

0 Instances 0%

vCPU Count

0 vCPUs 0%

RAM Usage

0 GB 0%

Floating IP Count

0 IPs 0%

VNFs

0 VNFs 0%

Add Tenant

Tenant Name

Domain: Default

Cloud User Name

User Password

Associated Cloud: RCO-1

Default/Default
<default user domain>/<optional project domain>

Cancel Save

The tenant is checked for proper configuration against the target VIM when the user clicks **Save**. A successful configuration of the tenant sends a notification and creates an entry in the Tenants panel on the Tenants screen.

If the configuration has an error, a notification appears in the top right of the screen and the Tenants panel remains available for editing.

5. Click **Save**. The tenant becomes available for use after the VNFM has retrieved associated quota limitations and OpenStack resource access.

Editing VNF Tenant Accounts

Use the following procedure to edit the VNF tenant account.

1. Log into the VNFM UI. See [Logging into the VNFM UI](#).
2. Select **VNFM Configuration>Tenants**.
3. In the Tenants panel, click on the tenant account to be edited.

Edit Tenant Panel

Tenants > Edit Tenant

OTT.PC2.VNFMDES.CIM.1

Tenant Usage

Live VNF Status: Totals

Instance Count (VNFs)
1/22 Instances 4%

vCPU Count
4/88 vCPUs 4%

RAM Usage
4/220 GB 1%

Floating IP Count
0/30 IPs 0%

VNFs
0/1000 VNFs 0%

Tenant Config

Tenant Name: OTT.PC2.VNFMDES.CIM.1

Domain: Default/Default

Cloud User Name: andrea

User Password:

Associated Cloud: Ottawa_PC2

Cancel Save

4. In the edit tenant panel, change the following as needed:
 - a. Edit the tenant name in the *Tenant Name* field. This name must match the OpenStack project name.
 - b. Edit the domain for the associated cloud in the *Domain* field. This name must match a domain from the OpenStack VIM in which the tenant is hosted. The default value is Default.
 - c. Edit the user name for the associated cloud in the *Cloud User Name* field. This name must match a user name from the OpenStack VIM in which the tenant is hosted, with permission to access that tenant.
 - d. Edit the password for the associated cloud in the *User Password* field. This must be the password associated with the Cloud User Name.

Note

The password field is not required to be edited. If you leave it empty, the old password remains for this user.

- e. Select the associated cloud from the *Associated Cloud* drop-down. This maps the project to its associated VIM instance. The tenant is checked for proper configuration against the target VIM when the tenant is added. A successful configuration of the tenant sends a notification and creates an entry in the Tenants panel on the Tenants screen. If the configuration has an error, a notification appears in the top right of the screen.

5. Click **Save**.

Deleting a VNF Tenant Account

Use the following procedure to delete a VNF tenant account.

1. Log into the VNF M UI. See [Logging into the VNF M UI](#).
2. Select **VNFM Configuration>Tenants**.
3. In the Tenants panel, click on the tenant to be deleted.
4. From the Select Action drop-down menu select **Delete**.

Delete a Tenant

Tenants

Add Tenant

Tenant (Project) ↑↓	Cloud User ↑↓	Cloud ↑↓	Instances ↑↓	vCPU ↑↓	RAM ↑↓	Floating IP ↑↓	VNFs ↑↓	Actions
RCO-PC1-2-EMS-AUTO.1	mhthuc	RCO-1	1%	7%	5%	0%	0%	
RCO-PC1-2-SV-VNFM-DSC.1	mhthuc	RCO-1	100%	65%	68%	0%	0%	Delete
RCO-PC1-2-SV-VNFM-EMS.1	mhthuc	RCO-1	66%	53%	62%	25%	0%	
RCO-PC1-2-SV-VNFM-GR	mhthuc	RCO-1	0%	0%	0%	0%	0%	
RCO-PC1-2-SV-VNFM-HA	mhthuc	RCO-1	0%	0%	0%	0%	0%	

1 - 5 of 6 << < 1 2 > >> 5

5. The Delete window appears.

Note

You will see an error informing that you cannot delete the tenant if the tenant:

- Currently has a VNF deployed by this VNFM, or
- Is assigned to a user as part of the Role-Tenant relationship. That tenant cannot be removed from the system until that Role-Tenant relationship is removed from any given user using the VNFM UI, that contains that Tenant.

Delete Confirmation

Delete

Are you sure you want to remove the tenant *OTT.SBCEMS.VNF.3* on cloud [Ottawa] from VNFM?
This action cannot be undone.

No

Yes

6. Click **Yes** to confirm the deletion of the tenant.

Onboard VNFs Using CSAR Packages

Additional Topics

- [Verify the VNFM State Before Onboarding VNF](#)
- [Perform Onboarding Through the UI](#)

To onboard the Ribbon Application Management Platform (RAMP) VNF on VNFM, refer to [Onboarding VNF Packages](#).

Verify the VNFM State Before Onboarding VNF

Check the VNFM status before onboarding the Ribbon Application Management Platform (RAMP) VNF. For more information, refer to [Verifying the VNFM and VNFM VM Status](#).

Perform Onboarding Through the UI

To onboard the Ribbon Application Management Platform (RAMP) VNF from the VNFM, refer to [Performing Onboarding Through the UI](#).

Instantiate a VNF

Perform the following procedure to instantiate the Ribbon Application Management Platform (RAMP) VNF on the VNFM.

Start

1. Log on to the VNFM.
2. Navigate to **VNF Catalog**. The **VNF Catalog** pane is displayed.
3. In the **Actions** column, click the menu in the RAMP row and then select **Instantiate**. The Instantiate VNF pane is displayed.
 - a. In the **VNF Name** field, enter the VNF Instance name.
 - b. From the **Cloud Name** menu, select the OpenStack Dashboard name.
 - c. From the **Tenant Name** menu, select the tenant name (that you created).
 - d. (Optional) From the **Zone** menu, select a zone name.
 - e. (Optional) From the **Continuity Plan** menu, select a Continuity Plan. For more information, refer to [Configuring Users, Roles, and Security Realms](#).
 - f. Click the **Network** pane and select the networks.
 - g. Click the **Address/Port** pane and select the ports.

Note

If the IPv6 address contains 7 octets, enter at least one digit for the all-zero group to make it 8 octets.

- **Incorrect:** 2607:f160:b:105a:cf:209::20
- **Correct:** 2607:f160:b:105a:cf:209:0:20

- h. (Optional) Click the **Flavor** pane.
 - i. From the **Available Flavors** menu, select a flavor.

Note

By default, RAMP selects the flavor from the VNFD.

- i. (Optional) Click the **Storage Volumes** pane.
 - i. Reuse a Cinder volume from one of the previous Orchestrations or attach the existing volume to VNFC instance.
 - ii. Select storage volume(s) to attach to VNFC instance(s).
- j. In the **VNF Specific** section, perform the following:
 - Without cinder boot disk:
 1. (Optional) In the **VNF Name** field, enter a name for the VNF. For hostname conventions, refer to [Hostname and Instance Name Conventions](#).
 2. In the **IP version ipv4/6** field, enter the IPv4 or IPv6 depending on your network.

3. (Optional) In the **NTPServer** field, enter the NTP server IP address. For example, [" fd00:10:6b50:4500::11 "," fd00:10:6b50:4500::12 "].
4. (Optional) In the **DNS Server** field, enter the DNS server.
5. (Optional) In the **Time Zone** field, enter the time zone.

If Time Zone is America_Network, the time zone in RAMP is UTC. If a specific time zone such as Asia/Kolkata is required then the Time Zone format should be Asia/Kolkata.

6. In the **LI Mediation Server TCP/SSL port** field, enter the Lawful Intercept Mediation Server port number.
7. In the **Number of Floating IPs** field, enter the number of floating IP addresses.
8. (Optional) In the **Interface Name prefix** field, enter "iscsi".
9. In the **Type of disk** field, enter "iscsi".
10. In the **Size of the volume** field, enter "90GB".
11. In the **Cloud Config Init Data** field, enter the following:

```
runcmd:
- usermod -p '<encrypted admin password>/' admin
users:
- name: insight
ssh_authorized_keys:
- <SSH key>
- name: admin
ssh_authorized_keys:
- <SSH key>
```

Note

For the GR target, pass the SSH keys from the RAMP source instance. It is applicable for admin and insight users.

For example:

```
runcmd:
- usermod -p '$6$BzdlFaNVC.etRjAZ$IDW8ytHjH2AlSNGwu5/
dnnLTV.gjbpTyMbSYguA.g.U1i0y9Bm3sKb8TKADo4UnFfzsqFWr67fNEfhnJVxTt0.' admin

users:
- name: insight
  ssh_authorized_keys:
    - ssh-rsa
    AAAAB3NzaC1yc2EAAAABIwAAAIEAvf4xCxJ7KCuskBsEeMtHEreEfv0n6Rc7SG6chSayooWl6q
    4RIRAPgVYm7UciMwxZy7bseQ1DJE2WkumA7kU0myvzsMfkXemXK63Uc7PWZMt2htHWAqn2As1Z
    fKchzprXWc2zGX7CfMELckr36SzqTjcQMzX+atyCpPP00L+uwNs= jklotzbach@insight
- name: admin
```



```

passwd: $6$BzdlFaNVC.etRjAZ$IDW8ytHjH2A1SNGwu5/
dnnLTV.gjbpTyMbSYguA.g.U1i0y9Bm3sKb8TKADo4UnFfzsqFwr67fNEfhnJVxTt0.
lock_passwd: false
ssh_authorized_keys:
- ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAvf4xCxJ7KCuskBsEeMtHEreEfv0n6Rc7SG6chSayooWl6q
4RIRAPgVYm7UciMwxZy7bseQ1DJE2WkumA7kU0myvzsMfkXemXK63Uc7PWZMt2htHWAqn2As1Z
fKchzprXWc2zGX7CfMELckr36SzqTjcQMzX+atyCp00L+uwNs= jklotzbach@insight

```

- Click **Instantiate**. The RAMP is instantiated under your new tenant in VNFM. The newly created RAMP VNF is displayed in the **VNF Lifecycle**.
The VNF status changes and the final status is Ready.
For managing RAMP VNF, refer to [VNF Orchestration and Lifecycle Management](#).

Migrate operations are not supported for RAMP VNFs with boot cinder-volume.

- Click the **VNF Information** pane and set the VNF configuration.

Post-RAMP Instantiation Tasks

Perform the following procedures after instantiating the Ribbon Application Management Platform (RAMP).

- [Obtain the RAMP SSH Keys](#)
- [Deploy MNP Services](#)

Installing RAMP on VMware Manually

Related articles:

- [System Requirements](#)
- [Checklist for Installing RAMP on VMware](#)
- [Deploy Optional Services on RAMP](#)
- [Configuring RAMP GR](#)
- [Configuring RAMP GR with Automatic Switchover Enabled](#)

You can install Ribbon Application Management Platform (RAMP) on VMware ESXi manually using the procedures outlined in this topic.

The workflow below provides an overview of the process and provides links to the specific information and steps required to complete installation. After completing the steps on a linked page, return to the workflow for the next procedure.

Step	Action
1	Review System Requirements to ensure your environment has the necessary resources and prerequisite software available.

Step	Action
2	Review the Checklist for Installing RAMP on VMware to ensure you have the network parameters to perform the installation process.
3	Download the following installation files to a Linux server. Refer to Download Files from Ribbon Support Portal for instructions for downloading files from Ribbon. • ramp-V<version>-RHEL-<version>.vmdk • configDriveImgDeployment.img • ramp-V<version>-RHEL-<version>.ovf For the list of installation files, refer to the Software Bundle section in the current RAMP release notes. Refer to Production Releases to access the release notes.
4	Either complete Install RAMP on VMware to create a standalone instance of RAMP. Or Perform the Install RAMP with VMware OVA Template Customization.
5	(Optional) If you plan to manage SBC Edge devices with RAMP, enable the EdgeView (EV) service. For more information, refer to Deploy Optional Services on RAMP .
6	(Optional) To configure RAMP in a GR deployment, you must create a second virtual machine instance to act as the Standby node in the GR pair. • Create the second instance following a similar process (recently completed) to create the initial instance. • While creating additional instances, use a different mount directory and another instance of the configDriveImgDeployment.img file. • After creating the second instance, refer to Configuring RAMP GR or Configuring RAMP GR with Automatic Switchover Enabled for the procedure to configure the two instances as a GR pair.
7	Install RAMP licenses. Refer to License Management .

After completing the installation process, refer to the [RAMP User Guide](#) for additional information on configuring and working with RAMP.

Checklist for Installing RAMP on VMware

Related articles:

- [Installing RAMP on VMware Manually](#)
- [System Requirements](#)
- [Install RAMP on VMware](#)

Before you install Ribbon Application Management Platform (RAMP) on VMware ESXi, you need to ensure you have the following:

- A Linux server on which you have root access to which you can download the RAMP installation files and where you can create an .ova file that you use during installation. This Linux server must have mount/vim/mkisofs installed.
- The login credentials for your ESXi WEB-UI environment.
- Details about your VMware datastore repository.
- Details about the port group (network mappings) you want to use for the instance.

Use the following table to assist you in gathering system information in preparation for installing RAMP on VMware ESXi. Ribbon recommends that you record these parameter values and have them available to use during the installation process and while configuring RAMP.

Installation Parameters for RAMP Standalone

Ribbon Network Configuration	Parameters	Description	Example Values	(M)andatory / (O)ptional
Hostname	Hostname	The name of the host system Refer to Hostname and Instance Name Conventions .	BLRRAMP01a	M
	Primary DNS	The primary DNS server IP address	10.9.9.97	O
	Secondary DNS	The secondary DNS Server IP address	10.9.9.98	O
	DNS Search Path	The domain name to resolve the IP address	eng.sonusnet.com	O
IP Configuration	Choose IP Format	The IP address format in IPv4 (default)	10.54.8.62 (IPv4 format)	M
	Available Ports	The primary network interface (PNI) from the available ports to assign to the system	eth0	M
	IP Address	The IP address for the selected network interface	10.54.8.62	M
	Netmask	The network mask	255.255.255.0	M
	Gateway	The gateway IP address of the network	10.54.8.1	M
Time Zone	Time Zone	The time zone	America/New York	M

Ribbon Network Configuration	Parameters	Description	Example Values	(M)andatory / (O)ptional
Time Server	Time Server	The NTP server IP address to synchronize the system time	10.128.245.36	M

Install RAMP on VMware

Related articles:

- [Installing RAMP on VMware Manually](#)
- [System Requirements](#)
- [Checklist for Installing RAMP on VMware](#)

Complete the following steps to create a standalone instance of Ribbon Application Management Platform (RAMP) on VMware ESXi. If you have not already done so, refer to [Installing RAMP on VMware Manually](#) for a workflow table outlining the installation process, including prerequisite steps to review system requirements, gather installation parameters, and download installation files.

Note

You must hold a Linux server, RHEL 7.8 or above, with the `mkisofs` package installed.

Start

1. Log on to the Linux server you downloaded the installation files onto. Ensure that the `ovf`, `.vmdk`, and `.img` files are available in the same directory.
2. Change to the directory containing the copied files:

Example:

```
cd /home/vmware_install
```

- a. Create a temporary mount directory:

```
mkdir -p /tmp/vmconf
```

- b. Mount the `configDriveImgDeployment.img` file to the temporary mount directory:

```
mount -o loop configDriveImgDeployment.img /tmp/vmconf
```

Note

To create multiple instances, use a different mount directory and `configDriveImgDeployment.img` file for each instance.

- c. Run the following command and use the information in the table to modify the `configDriveImgDeployment.img` file for your deployment. By default, the template file has two interfaces: IF1 and IF2. Use the IF2 interface when to enable Secondary Management Interface.

vim /tmp/vmconf/user-data			
Key Name	Description	Mandatory (M) / Optional (O)	Example Value
timezone	The Time Zone for your network in which the VM is created.	M	Asia/Kolkata
ntpServer	The NTP server IP address if you have an NTP server. To add multiple NTP servers (up to 5 allowed), enter the NTP server IP addresses in the following format: Servers: \$ntpServer1 \$ntpServer2 \$ntpServer3 \$ntpServer4 \$ntpServer5	M	<pre>servers: - 10.128.254.67 - 10.128.254.68 - 10.10.211.119</pre>
dnsServer	The IP address of the DNS server.	O	- IPV4: 10.128.254.67 - IPV6: 0:0:0:0:ffff:c0a8:101
dnsSearchPath	The search path for the DNS server.	O	rbbn.com

Key Name	Description	Mandatory (M) / Optional (O)	Example Value
InstanceName	The RAMP instance or Virtual Machine (VM) name. The InstanceName criteria: • Uppercase or lowercase letters [a-z], [A-Z] • Digits [0-9] • Do not begin the name with a digit. • Do not use special characters, including the hyphen.	M	ramp SA
instance-type	The RAMP installed on the non-cloud (KVM/VMware).	M	non-cloud
MGT1	Note: This flag is set to N. Change it to Y to use the Secondary MGT Interface. If MGT1 is configured, you cannot configure Lawful Interface (LI). Note By default, MGT1 is set to N. When MGT1 is mandatory, or the flag is set to Y, the IF2 values get populated.	O	Y
IF1			
GWV4	Note: This parameter is applicable only if you are creating a RAMP VM in an IPv4 network. The gateway IP address from the available network pool in IPv4.	M	192.168.1.1
IPV4	Note: This parameter is applicable only if you are creating a RAMP VM in an IPv4 network. The fixed management IPV4 address for the interface. • IF1Ipaddr is the IP address of eth0	M	192.168.1.7/24

Key Name	Description	Mandatory (M) / Optional (O)	Example Value
GWV6	Note: This parameter is applicable only if you are creating a RAMP VM in an IPv6 network. The gateway IP address from the available network pool in IPv6.	O	0:0:0:0:ffff:c0a8:101
IPV6	Note: This parameter is applicable only if you are creating a RAMP VM in an IPv6 network. The fixed management IPV6 address for the interface and netmask. • IF1paddrv6 is the IP address of eth0	O	0:0:0:0:ffff:c0a8:107/64
IF2			
GWV4	Note: This parameter is applicable only if you are creating a RAMP VM in an IPv4 network. The gateway IP address from the available network pool in IPv4.	M	192.168.1.1
IPV4	Note: This parameter is applicable only if you are creating a RAMP VM in an IPv4 network. The fixed management IPV4 address for the interface. • IF2Ipaddr is the IP address of eth1	M	182.168.1.7/24
GWV6	Note: This parameter is applicable only if you are creating a RAMP VM in an IPv6 network. The gateway IP address from the available network pool in IPv6.	O	0:0:0:0:ffff:c0a8:101
IPV6	Note: This parameter is applicable only if you are creating a RAMP VM in an IPv6 network. The fixed management IPV6 address for the interface and netmask. • IF2paddrv6 is the IP address of eth1.	O	0:0:0:0:ffff:c0a8:107/64

Example

```
path: /opt/rbbn/userData.json
```

```
permissions: '0644'
content: |
{
  "IF1": {"GWV4": "$gww4", "IPV4": "$ipv4/$prefix", "Port": "eth0"},
  "IF2": {"GWV4": "", "IPV4": "/", "Port": ""},
  "growpart": { "opt" : 60, "pgsql": 30, "home":10},
  "instance-type": "non-cloud",
  "InstanceName": "$instanceName",
  "MGT1": "N" # Make it "Y" when using Secondary MGT Interface
}
```

If MGT1 is set to Y:

Example

```
path: /opt/rbbn/userData.json
permissions: '0644'
content: |
{
  "IF1": {"GWV4": "$gww4", "IPV4": "$ipv4/$prefix", "Port": "eth0"},
  "IF2": {"GWV4": "$gww4", "IPV4": "$ipv4/$prefix", "Port": "eth1"},
  "growpart": { "opt" : 60, "pgsql": 30, "home":10},
  "instance-type": "non-cloud",
  "InstanceName": "venus2ramp",
  "MGT1": "Y"
}
```

- d. (Optional) If your internal network is clashing with the networks created by the docker service, add the file `/opt/rbbn/dockerNetworksFile` through the user-data or the HEAT template. This file validates and writes the data to the `/etc/docker/daemon.json` file. For more information on Docker Daemon, refer to [RAMP Customisation for Docker Daemon](#).

Note

At times, the internal network assigned by the docker service is the same as the network used in your premises. This leads to a conflict in the network and connectivity issues. In such a scenario, specify the docker service to pick the provided IP Address from the pool for the docker internal network.

Note

You must add a minimum of seven networks for the RAMP 24.06 release. You are allowed to add networks that suit you but do not change the variable names.

IPV6 support is currently disabled.

Example

```

write_files:
  - path: /opt/rbbn/dockerNetworksFile
    permissions: '0744'
    owner: root:root
    content: |
      dockerNetwork1=172.21.0.0/16
      dockerNetworkSize1=24
      dockerNetwork2=172.22.0.0/16
      dockerNetworkSize2=24
      dockerNetwork3=172.23.0.0/16
      dockerNetworkSize3=24
      dockerNetwork4=172.24.0.0/16
      dockerNetworkSize4=24
      dockerNetwork5=172.25.0.0/16
      dockerNetworkSize5=24
      dockerNetwork6=172.26.0.0/16
      dockerNetworkSize6=24
      dockerNetwork7=172.27.0.0/16
      dockerNetworkSize7=24

```

Example of created user data

```

#cloud-config
timezone: "Asia/Kolkata"
ntp:
  enabled: true
  ntp_client: chrony
  config:
    conffpath: /etc/chrony.conf
    check_exe: chronyd
    packages:
      - chrony
    service_name: chronyd
    template: |
      ## template:jinja
      # My NTP Client config
      {%- if servers %}# servers
      {% endif %}
      {% for server in servers -%}
      server {{server}} iburst
      {% endfor %}
    servers:
      - 10.128.254.68
manage_resolv_conf: true
resolv_conf:
  nameservers: ['8.8.8.8']

```

```

searchdomains:
  - $dnsSearchPath
write_files:
  - path: /opt/rbbn/userData.json
    permissions: '0644'
    content: |
      {
        "IF1": {"GWV4": "10.220.200.2", "IPV4": "10.220.200.168/24", "Port": "eth0"}
      },
      "growpart": { "opt" : 60, "pgsql": 30, "home":10},
      "instance-type": "non-cloud",
      "InstanceName": "RAMP01"
      "MGT1": "N"
    }
  owner: root:root
  - path: /opt/rbbn/dockerNetworksFile
    permissions: '0777'
    content: |
      dockerNetwork1=172.21.0.0/16
      dockerNetworkSize1=24
      dockerNetwork2=172.22.0.0/16
      dockerNetworkSize2=24
      dockerNetwork3=172.23.0.0/16
      dockerNetworkSize3=24
      dockerNetwork4=172.24.0.0/16
      dockerNetworkSize4=24
      dockerNetwork5=172.25.0.0/16
      dockerNetworkSize5=24
      dockerNetwork6=172.26.0.0/16
      dockerNetworkSize6=24
      dockerNetwork7=172.27.0.0/16
      dockerNetworkSize7=24
    owner: root:root
  runcmd:
    - usermod -p '$1$admin$1kgWpnZpUx.vTrowPXPIB0' admin
    - usermod -f -1 admin

```

- e. Save and close the configuration file.
- f. Create the config drive ISO file from the mount point:

```
mkisofs -o configDriveImgDeployment.iso -V cidata -r -J /tmp/vmconf/
```

- g. Unmount the image:

```
umount /tmp/vmconf
```

- h. Delete the temporary mount point:

```
rm -rf /tmp/vmconf
```

3. (Optional) Edit the OVF template file to modify the default vCPU configuration. The following is an excerpt from an example OVF template file. You can edit the `VirtualQuantity` parameter to create a RAMP

instance with a different number of vCPUs.

Example

```
<Item>
<rasd:AllocationUnits>hertz * 10^6</rasd:AllocationUnits>
<rasd:Description>Number of Virtual CPUs</rasd:Description>
<rasd:ElementName>virtual CPU(s)</rasd:ElementName>
<rasd:InstanceID>1</rasd:InstanceID>
<rasd:Reservation>2900</rasd:Reservation>
<rasd:ResourceType>3</rasd:ResourceType>
<rasd:VirtualQuantity>16</rasd:VirtualQuantity>
```

- a. To support the eth1 (IF2) interface in the OVF template file, uncomment below Config in OVF file when trying to bring up RAMP with MGT1 interface.:

Example:

Network description

```
<!--Network ovf:name="Secondary Management Network">
  <Description>The Secondary management network for Application</Description>
</Network-->

<!--Item>
<rasd:AddressOnParent>8</rasd:AddressOnParent>
<rasd:AutomaticAllocation>true</rasd:AutomaticAllocation>
<rasd:Connection>Secondary Management Network</rasd:Connection>
<rasd:Description>VmxNet3 ethernet adapter on "Secondary Management Network"</
rasd:Description>
<rasd:ElementName>Ethernet 2</rasd:ElementName>
<rasd:InstanceID>9</rasd:InstanceID>
<rasd:ResourceSubType>VmxNet3</rasd:ResourceSubType>
<rasd:ResourceType>10</rasd:ResourceType>
</Item-->
```

4. Create the manifest file:

```
openssl sha256 OVF_FILE_NAME.ovf VMDK_FILE_NAME.vmdk > MANIFEST_FILE_NAME.mf
```

Example

```
openssl sha256 ramp-V22.06.00R00-RHEL-8.5.20-x86_64_68.ovf ramp-V22.06.00R000-RHEL-8.5.20-x86_64_68.vmdk > ramp-V22.06.00R000-RHEL-8.5.20-x86_64_68.mf
```

5. Create the ova tar file by bundling the .ovf, .vmdk, and .mf files:

```
tar cf ramp-V<version>-RHEL-<version>.ova ramp-V<version>-RHEL-<version>.ovf ramp-V<version>-RHEL-<version>.vmdk ramp-V<version>-RHEL-<version>.mf
```

Example

```
tar cf ramp-V22.06.00R00-RHEL-8.5.20-x86_64_68.ova ramp-V22.06.00R00-RHEL-8.5.20-x86_64_68.ovf ramp-V22.06.00R00-RHEL-8.5.20-x86_64_68.vmdk ramp-V22.06.00R00-RHEL-8.5.20-x86_64_68.mf
```

6. Launch the VM:

- a. Copy the `.ova` and `.iso` files to the local computer/remote desktop.
- b. Log on to the ESXi WEB-UI.
- c. Upload the `.iso` (`configDriveImgDeployment.iso`) file to the datastore:
 - i. Click **datastore** in the navigation pane.
 - ii. Navigate to the **Datastore browser**.
 - iii. Create a destination directory for the uploaded file, example: `VMware_22_06`
 - iv. Browse and select the `configDriveImgDeployment.iso` file.
 - v. Click **Upload**.
 - vi. Click **Close** to close the **Database browser**.
- d. Click **Virtual Machines** in the navigation pane.
- e. Navigate to **Create / Register VM**.
- f. Click **Deploy a virtual machine from OVF or OVA file**.
- g. Click **Next**.
- h. Enter the name of the VM.
 - i. Drag and drop/browse for the `.ova` file.
 - j. Click **Next**.
- k. Select the storage for VM.
 - l. Click **Next**. This step extracts the `.ova` file.
- m. Select the appropriate network.
- n. Select Disk provisioning as **Thick provisioned, lazily zeroed**.
- o. Clear the checkbox "Power on automatically".
- p. Click **Next**.
- q. Click **Finish**.
- r. Wait for the upload to complete.
- s. Once the upload is complete, right-click on the VM and select **Edit settings**.
- t. In the **CD/DVD Media** field, select the **Datastore ISO file** from the dropdown list. Browse and select the `configDriveImgDeployment.iso` file, that was uploaded to the datastore.

Note

Enable the Connect at Power status.

- u. Click Add Network Adaptor and select the adaptor to connect.

Add the adaptor only when MGMT1 is Y.

- v. Click **Save**.

7. Power on the VM. The VM boots up, and the system automatically configures it using the config drive.
8. Wait at least 10 minutes for the previous step to complete, and then ssh to **RAMP** as the admin user. The default admin password is "admin". To change the password, refer to [Manage RAMP Account Names and Passwords](#).
9. Check **RAMP** status. For more information, refer to [Check RAMP Status](#).

10.

Note

This step is only required if the RAMP VM is set up with the VM Options tab/VMware Tools: Time 'Synchronize guest time with host' selected (it is cleared by default). When enabled, alter the VMX configuration to prevent VMware from interfering with the time sync with the RAMP since RAMP uses its internal time server.

- a. Log on to the VMware host.
- b. Shutdown the RAMP guest instance. For example, if the name of the RAMP guest instance is **hefeweizenjtc1**, then shutdown **hefeweizenjtc1**.
- c. Navigate to the location of the VMX file and edit it. An example of the path where the file is stored: `/vmfs/volumes/datastore1/<hefeweizenjtc1>/hefeweizenjtc1.vmx`.
- d. Append the following lines in to the VMX file::

Note

```
time.synchronize.continue = "FALSE"
time.synchronize.restore = "FALSE"
time.synchronize.resume.disk = "FALSE"
time.synchronize.shrink = "FALSE"
time.synchronize.tools.startup = "FALSE"
time.synchronize.tools.enable = "FALSE"
time.synchronize.resume.host = "FALSE"
```

- e. Save the VMX file and start the VM.
11. Return to the workflow table on [Installing RAMP on VMware Manually](#).

Install RAMP with VMware OVA Template Customization

In this section:

- [Create Customization Specification](#)
- [Create RAMP Template](#)
- [Create RAMP VM from RAMP Template](#)
- [Create RAMP Config Drive ISO](#)

The Ribbon Application Management Platform (RAMP) supports installing RAMP using VMware OVA Template customization.

Prerequisite

Perform the initial configuration based on [Installing RAMP on VMware Manually](#).

Create Customization Specification

Use this procedure to customize specifications for the Virtual Machine (VM):

Start

1. Log on to the vSphere client as administrator.
2. Select the **Policies and Profiles** page from the menu.
3. Click **New** under VM Customization Specifications.
4. In the **New VM Customization Specification** window, provide a **Name** and **description**, and select the **vCenter Server**.
5. Select **Linux** as the Target guest OS and click **NEXT**.
6. In the **Computer name** screen, select the **Use the virtual machine name** and click **NEXT**.
7. Select the **Area**, **Location**, and **Hardware clock set to** as appropriate and click **NEXT**.
8. In the **Network** screen, select **Manually select custom settings** and add a total of 1 NIC for RAMP. Click **NEXT**.
9. In the **DNS Settings** screen, select **Prompt the user for an IPv4 address when the specification is used** and click **NEXT**.
10. Provide the **Primary DNS**, **Secondary DNS**, and **Tertiary DNS server** information in the **DNS settings** page and click **NEXT**.
11. Click **FINISH** in the **Ready to Complete** screen, to create customization specifications.

Create RAMP Template

Perform the following procedure to create an OVA file for RAMP using the downloaded `vmdk` and `ovf` files:

Start

Note

To create an OVA template, perform steps 3 to 5 from [Install RAMP on VMware](#).

1. Log on to the vSphere client as `admin` user.
2. Select **Deploy OVF Template** to create the VM template from the OVA package.
 - a. Select **RAMP OVA package** via URL or Local File.
 - b. In the **Select an OVF template** window, click **UPLOAD FILES** to upload the OVA files. Click **NEXT**.

- c. Enter the VM name in the template and click **NEXT**.
- d. Select the destination computer resource and review the details. Click **NEXT**.
- e. Select the storage and VM storage policy. Click **NEXT**.
- f. Select the Networks and click **NEXT**.
- g. In the **Ready to Complete** screen, click **FINISH**.
The VM is created.
3. Click the VM and select **Edit Settings**.
4. Check the guest OS version and continue to the next step if it is RHEL 8. If it is not RHEL 8, edit the guest OS version to **RHEL 8 (64-bit)** under the **VM Options** tab.

Note

RHEL 8 is not available due to compatibility of VMWare Esxi as it should be 6.7 and above.

5. Navigate to your VM and select **Template > Convert to Template**.

Create RAMP VM from RAMP Template

Perform the following procedure to create a RAMP VM from the RAMP template:

Start

1. Log on to the vSphere client as `admin` user.
2. Choose any template and select **New VM from This Template** option.
3. Follow the steps to create a new VM from that template.
 - a. Specify the VM Name. Click **NEXT**.
 - b. From the **Select storage** screen, select the host and datastore. Click **NEXT**.
 - c. In the **Select clone options** screen, select the **Customize the operating system** option and click **NEXT**.
 - d. In the **Customize guest OS** section, select **rampspecification** and click **NEXT**.
 - e. In the **User Settings**, enter the IP address, Netmask and Gateway for management interface of RAMP. Click **NEXT**.
 - f. Click **Finish**. The RAMP VM is created.
4. Click the **Power On** icon to switch on the VM.
5. Check **Events** under **Monitor** tab to ensure that the customization specification is applied successfully.
6. Log on as `admin` user or try to SSH into VM using `admin user` and **management IP address**.
7. Log on as a `root` user.
8. Reset the admin password back to admin using:

```
# passwd admin
```

Create RAMP Config Drive ISO

Perform the following steps to create a configDrive ISO on a third Server. This can be mounted into RAMP using ansible Playbook.

1. Create config drive ISO for the RAMP VM.
2. Use the `configDriveImg.img` file downloaded from the artifactory.

When the `configDriveImg.img` is mounted, you get two files, user-data and meta-data files. Edit the meta-data file so that `{}` is replaced by **`dsmode:local`**.

Note

Create the config drive using steps 1 and 2 in [Install RAMP on VMware](#) for creating the config drive.

Note

The IP Address provided while creating `ConfigDrive` is same as the one provided while creating the VM from Template.

3. After creating the `configDrive`, copy the `ConfigDrive` to RAMP.
4. Log on to the RAMP as an `admin` user.
5. Change to `root` user:

```
sudo su -
```

Note

RAMP has the `vmwarecustomization` (`vmware-customization.tar.gz`) files required for running ansible on the folder `/opt`.

6. Untar the **`vmware-customization.tar.gz`** into a folder where `ConfigDrive` is available.
7. Edit the hosts files with `src_path`:

```
all:
  hosts:
    vmwareNode1:
      ansible_host: "localhost"
      ansible_user: "admin"
      src_path: "/home/admin/configDriveImgDeployment.iso"
```

8. Set hosts file path in `ansible.cfg` file.

```
inventory=/home/admin/hosts
```


While running Ansible playbook the below warning is displayed, but this can be ignored.

```
/opt/sonus/ems/.local/lib/python3.8/site-packages/paramiko/
transport.py:219: CryptographyDeprecationWarning: Blowfish has been
deprecated and will be removed in a future release
  "class": algorithms.Blowfish,
/usr/lib/python3.8/site-packages/requests/__init__.py:89:
RequestsDependencyWarning: urllib3 (2.1.0) or chardet (3.0.4) doesn't
match a supported version!
  warnings.warn("urllib3 ({}), or chardet ({}), doesn't match a supported
"
```

9. Set python path to `python3.6` :

```
export PYTHONPATH=/usr/lib/python3.6/site-packages/
```

10. Trigger the ansible-playbook:

```
ansible-playbook vmware-playbook.yml --connection=local
```

When ansible playbook is successful, the RAMP takes up to 15 mins to come up into service.

11. Use the commands `emsMgmt` and `emsProcMgmt.log` to check the status of `cloud-init status`, `og /var/log/cloud-init.log` and the application status.

VMotion on VMware for RAMP

In this section:

- [Setup RAMP on vSphere Client](#)
 - [Create a Cluster](#)
 - [Add Hosts to the Cluster](#)
 - [Configure the Cluster \(Quickstart\)](#)
 - [Deploy RAMP](#)
 - [Configure the Virtual Machine](#)
 - [Migrate Using vMotion](#)

The Ribbon Application Management Platform (RAMP) supports VMotion to migrate multiple virtual machines from one server to another.

Prerequisite

Refer to [Installing RAMP on VMware Manually](#) for initial configuration.

Setup RAMP on vSphere Client

Create a cluster to setup RAMP on a vSphere client.

Create a Cluster

Perform this procedure to create a cluster.

Start

1. Log on to the vSphere client as `admin` user.
2. Create a cluster:
 - a. Click **Datacenter**.
 - b. Select **New Cluster**.
The "New Cluster" dialog displays.
 - c. In the **Basics** tab on the right pane, provide a name for the cluster to create in the **Name** field.
 - d. Enable **vSAN**.
 - e. Click **Next**.
The "Review" dialog displays.
 - f. Review the details for the cluster and click **Finish**.
A new cluster is created.

Add Hosts to the Cluster

Hosts are allowed to be added to the cluster on successful cluster creation. Perform the following procedure to add hosts to the created cluster.

Start

1. Right click on the cluster and select **Add Hosts**.
The "Add Hosts" dialog displays.
2. Enter the Host IP Address, username, and password.
3. Click **ADD HOST**.
4. Click **Next**. The **Host summary** dialog displays.
5. Verify the details and click **Next**.
The "Review and Finish" dialog displays.
6. Review the details and click **Finish**.

Configure the Cluster (Quickstart)

Perform the following procedure to configure the cluster.

Start

1. Ensure all the hosts are in maintenance mode.
2. Configure the D-Switch.
3. Select the **vswitch0** adapter.
4. Select **Static IP Allocation**.

5. Provide the **Host Address** details with the respective **Subnet Mask** and **Gateway IP Address**.
For example, Host Address: 10.228.40.40, Subnet Mask: 255.255.254.0, and Gateway IP Address: 10.228.40.1.
6. Review the distributed switch.
7. Click **Finish**.

Deploy RAMP

Perform the following procedure to deploy RAMP.

Start

1. Right click on any host in the cluster to deploy RAMP.
2. Select **Deploy OVF Template**.
The "Deploy OVF Template" dialog displays.
3. Select **Local File** in the "Select an OVF Template" dialog.
4. Click **Upload Files** to upload the `.ova` file from the local directory.
5. Click **Next**.
The "Select a name and folder" pane displays.
6. Provide a name in the **Virtual machine name** field.
7. Click **Next**.
The "Select a compute resource" pane displays.
8. Select the destination compute host to deploy RAMP.
9. Check the **Compatibility** field for the presence of a 'compatibility checks succeeded' message.
10. Click **Next**.
The "Review details" pane displays.
11. Review the details of the resources and click **Next**.
The "Select Storage" pane displays.
12. Select **vsanDatastore**.
13. Select a compatible **VM Storage Policy**.
14. Check the **Compatibility** field for the presence of a 'compatibility checks succeeded' message.
15. Click **Next**.
The "Select Networks" tab displays.
16. Select the destination management network.
17. Click **Next**.
The "Ready to complete" pane displays.
18. Review the details and click **Finish**.
19. Verify RAMP installation on the host.
20. Right click on the newly created RAMP and select **Edit Settings**.
The "Edit Settings" dialog displays.
21. Navigate to **Virtual Hardware > CD/DVD drive 1** and select **Datastore ISO File**.
22. In the "CD/DVD Media" pane, click **Browse** to choose the `.iso` file and click **OK**.
23. Enable **Connect At Power On**.
24. Select **VM Options**.
25. Select **Linux** as the **Guest OS**.
26. Select the **Guest OS Version**.
27. Click **OK**.
28. Launch the web console to verify RAMP deployment.

Configure the Virtual Machine

Perform the following procedure to configure the virtual machine (VM).

Start

1. Right click on the newly created RAMP.

2. Select **Settings**.
3. Select the **Guest OS** Version.
4. Connect to the datastore `.iso`.

Note

Ensure the respective `.iso` file is uploaded to the datastore and available.

5. Click **Save**.

Migrate Using vMotion

Perform the following procedure to migrate RAMP from one host to another using vMotion.

Start

1. Right click on the RAMP to be migrated and select **Migrate**.
The "Migrate" dialog displays.
2. In the "Select a migration type pane", select **Change Compute resource only**.
3. Click **Next**.
The "Select a compute resource" pane displays.
4. Select the target host to perform vMotion.
5. Check **Compatibility** field for the presence of a 'compatibility checks succeeded' message.
6. Click **Next**.
The **Select storage pane** displays.
7. Select the appropriate **VM Storage Policy** and **vSANDatastorage**.
8. Click **Next**.
The "Select networks" pane displays.
9. Select the **D-Switch Management network of the target host**.
10. Check **Compatibility** field for the presence of a 'compatibility checks succeeded' message.
11. Click **Next**.
The "vMotion priority" pane displays.
12. Select **Schedule vMotion with high priority (recommended)**.
13. Click **Next**.
The "Ready to complete" pane displays.
14. Review the information and click **Finish** to start migration.
The vMotion progress displays.

The status changes to **Completed** once the migration completes.

Verify the migration of RAMP to the target host.

Installing RAMP in Public Cloud Environments

In this section:

- [Installing RAMP on AWS Manually](#)
 - [Create Security Groups and Security Group Rules on AWS](#)
 - [Create a Volume on AWS](#)
 - [Generate SSH Keys for RAMP Users on AWS](#)
 - [Copy RAMP SSH Keys to an External Server](#)
 - [Checklist for Installing RAMP on AWS](#)

- [Instantiate a Standalone RAMP Instance on AWS with Public IP Address](#)
- [Instantiate a Standalone RAMP Instance on AWS with Private IP Address](#)
- [Allocate an Elastic IP Address](#)
- [Installing RAMP on Azure Manually](#)
 - [Upload the RAMP Template to Azure](#)
 - [Create a Resource Group for RAMP on Azure](#)
 - [Create a Network Security Group for RAMP on Azure](#)
 - [Create an External Disk for RAMP on Azure](#)
 - [Generate SSH Keys for RAMP Users on Azure](#)
 - [Checklist for Installing RAMP on Azure](#)
 - [Instantiate a Standalone RAMP Instance on Azure](#)
 - [Create a New or Select an Existing Resource for Virtual Network](#)
 - [Create a Public IP Address](#)
 - [Generate Output Payload from createUIDefinition Sandbox](#)

Installing RAMP on AWS Manually

You can manually install Ribbon Application Management Platform (RAMP) in an Amazon Web Services (AWS) environment using the procedures outlined in this topic. RAMP uses the AWS CloudFormation service and a Cloud Formation template to facilitate installing RAMP on AWS. For more information on service and templates, refer to <https://aws.amazon.com/cloudformation>.

Note

Cross-platform support is not available for AWS. You cannot register devices brought up on other platforms (for example, Azure) to RAMP on AWS.

The workflow below provides an overview of the process and provides links to the specific information and steps required to complete installation. After completing the steps on a linked page, return to the workflow for the next procedure.

Step	Action	Procedure/Instructions
1	Review System Requirements to ensure your environment has the necessary resources and prerequisite software available.	System Requirements

Step	Action	Procedure/Instructions
2	Download the Cloud Formation template file from the Support Portal. Select the file based on your requirements. • RAMP with a private IP – Download <code>RAMP_AWS_CF_PRIVATE_TEMPLATE.yaml</code>. • The private IP is employed when the Virtual Network gateway for VPN is accessible within the On-prem lab, and ExpressRoute is set up on their On-prem network. • RAMP with a public IP – Download <code>RAMP_AWS_CF_PUBLIC_TEMPLATE.yaml</code>. The public IP possesses a public IP address along with a private IP address, making it usable when RAMP needs to be accessible over the Internet. For migrating from EMS to RAMP, use only the <code>RAMP_AWS_CF_PRIVATE_TEMPLATE.yaml</code> as EMS only supports a Private IP on AWS.	Download Files from Ribbon Support Portal
3	Allocate an external IP if you have chosen <code>RAMP_AWS_CF_PUBLIC_TEMPLATE.yaml</code> and configure RAMP with a public IP.	Allocate an Elastic IP Address
4	(Optional) Create a placement group that specifies the strategy you want to follow in deploying instances in your AWS environment. You have the option to specify the name a placement group when you instantiate RAMP. Refer to Amazon EC2 documentation for more information on placement group strategies and the steps to create a placement group using the EC2 Management Console.	Amazon EC2 documentation
5	Create a security group that contains security group rules for your RAMP instance.	Create Security Groups and Security Group Rules on AWS
6	Create a volume for your RAMP instance.	Create a Volume on AWS
7	Generate SSH keys to inject for the RAMP insight and admin users to enable password-less access.	Generate SSH Keys for RAMP Users on AWS

Step	Action	Procedure/Instructions
8	Review the Checklist for Installing RAMP on AWS to ensure you have the parameter values you will need during installation.	Checklist for Installing RAMP on AWS
9	To instantiate a standalone instance of RAMP, complete one of the following: • Instantiate a Standalone RAMP Instance on AWS with Private IP Address • Instantiate a Standalone RAMP Instance on AWS with Public IP Address	Installing RAMP on AWS Manually
10	(Optional) If you plan to manage SBC Edge devices with RAMP, enable the EdgeView (EV) service.	Deploy Optional Services on RAMP
11	Install RAMP licenses.	License Management

After completing installation, refer to the RAMP [RAMP User Guide](#) for additional information on configuring and working with RAMP.

Create Security Groups and Security Group Rules on AWS

In this section:

- [Create Security Group and Security Group Rules](#)
 - [Inbound Security Group Rule Port Descriptions](#)
 - [Route Table Rule](#)
- [Dynamic Host Configuration Protocol \(DHCP\) Option Set](#)

Related articles:

- [Installing RAMP on AWS Manually](#)
- [Checklist for Installing RAMP on AWS](#)
- [Instantiate a Standalone RAMP Instance on AWS with Public IP Address](#)

Prior to launching a Ribbon Application Management Platform (RAMP) instance on Amazon Web Services (AWS), create a security group. A security group is comprised of security group rules and acts as a virtual firewall to control incoming and outgoing traffic to an instance. Inbound rules control the incoming traffic to your instance, and outbound rules control the outgoing traffic from your instance.

You can modify the rules for a security group at any time. Any new and modified rules are automatically applied to all instances that are associated with the security group.

Note

If you are installing RAMP for the first time, you must create a security group to allow HTTPS access.

Create Security Group and Security Group Rules

Note

Before creating security group rules, create a subnet for this purpose within the virtual private cloud (VPC). Use the CIDR value for this subnet when creating security group rules.

To create a security group and security group rules for RAMP on Amazon Web Services (AWS), access the Amazon EC2 console. Refer to the [Amazon EC2 User Guide for Linux Instances](#) for the specific procedures. Use the information in the following tables to create security group rules for the subnet associated with the RAMP instance. Customize the security group as needed based on your network security requirements.

After creating the security group, enter the security group name when customizing the parameters (InstanceSecurityGroup) in the CloudFormation template during the process of instantiating your RAMP instance.

Inbound Security Group Rule Port Descriptions

Ribbon recommends to open the following ports using Inbound/Ingress rules in the security groups associated with the management interface.

For a complete list of RAMP ports, refer to [RAMP Ports Descriptions](#).

Inbound Ports

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Management IP of devices	Secure login to RAMP from a console terminal through SSH.
Custom UDP Rule	UDP	123	Management IP of devices	Network Time Protocol for clock synchronization. This is optional and only required when using an external NTP server.
Custom UDP Rule	UDP	161	Management IP of devices	SNMP reachability polling for the RAMP node.
Custom UDP Rule	UDP	162	Management IP of devices	SNMP Event notification V2 trap from other devices to RAMP.

Type	Protocol	Port Range	Source	Description
HTTPS	TCP	443	Management IP of devices	Redirects requests to JBoss application server, the RAMP Web GUI, SOAP and REST APIs.
Custom UDP Rule	UDP	5200	Management IP of devices	Agent trap receiver port used for receiving hardware traps sent from port 1610.
Custom TCP Rule	TCP	5432	Management IP of devices	PostgreSQL database – internal DB connections.
Custom TCP Rule	TCP	6462	Management IP of devices	Used for enabling FTP statistics collection from RAMP.
Custom TCP Rule	TCP	8122	Management IP of devices	Remote access to the RAMP CLI from a client through SSH.
Custom TCP Rule	TCP	9001	Management IP of devices	Client/server communication from PSX Manager to RAMPt through a PSX proxy server over HTTPS (SSL).
Custom UDP Rule	UDP	9004	Management IP of devices	Call Trace event notification from other devices to RAMP.
All ICMP - IPv4	All	N/A	Management IP of devices	
All traffic	All	All	Public management IP of RAMP	This is required only when RAMP is instantiated with public IP address.

Outbound Ports

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Management IP of devices	Connection (Tunneled protocols such as PIPE and so on).
Custom UDP Rule	UDP	123	Management IP of devices	Network Time Protocol for clock synchronization.
Custom UDP Rule	UDP	161	Management IP of devices	SNMP reachability polling for the RAMP node.

Type	Protocol	Port Range	Source	Description
Custom UDP Rule	UDP	162	Management IP of devices	SNMP event notification V2 trap from other devices to RAMP.
HTTPS	TCP	443	Management IP of devices	RAMP GUI access.
Custom TCP Rule	TCP	444	Management IP of devices	SBC platform port, used for inventory collection.
Custom UDP Rule	UDP	514	Management IP of devices	syslogd.
Custom UDP Rule	UDP	1812	Management IP of devices	Radius authentication port (configurable - this is the default).
Custom TCP Rule	TCP	2022	Management IP of devices	NETCONF sessions to SBCs.
Custom TCP Rule	TCP	2024	Management IP of devices	SFTP to SBC.
Custom TCP Rule	TCP	6462	Management IP of devices	RAMP and PSX communication (SFTP stats collection) using REST.
Custom TCP Rule	TCP	19991	Management IP of devices	Sonus agent configuration
All ICMP - IPv4	All	N/A	Management IP of devices	
All traffic	All	All	Public management IP of RAMP	This is required only when RAMP is instantiated with public IP address.

Route Table Rule

AWS uses the most specific route in your route table that matches the traffic to determine how to route the traffic (longest prefix match). You must either add a rule to route all the non-Virtual Private Clouds (VPC) traffic to an internet gateway, or ensure that the internet traffic is routed through your own NAT instance or gateway.

For example, the following route table has a route for IPv4 Internet traffic 0.0.0.0/0 that points to an Internet gateway. RAMP uses the Local route (routed within the VPC) to cover any traffic destined for a target within the VPC (10.0.0.0/16). All other traffic from the subnet uses the internet gateway.

Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-11aa22bb

For detailed information on the Route Table, refer to [AWS documentation](#).

Dynamic Host Configuration Protocol (DHCP) Option Set

The Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP/IP network. The `options` field of a DHCP message contains the configuration parameters. Some of those parameters are the domain name, domain name server, and the netbios-node-type.

The DHCP options sets are associated with your AWS account so that you can use them across all of your VPC. For detailed information on the DHCP option sets, refer to [DHCP Options Sets](#) in the AWS documentation.

The following DHCP option sets are provided by AWS:

- default DHCP option set
- custom DHCP option set

When you create a VPC, AWS automatically creates a set of DHCP options and associates them with the VPC. This set includes two options:

- `domain-name-servers=AmazonProvidedDNS`
- `domain-name=domain-name-for-your-region`

The `AmazonProvidedDNS` is an Amazon DNS server, which enables DNS for instances that need to communicate over the VPC's Internet gateway. The string `AmazonProvidedDNS` maps to a DNS server running on a reserved IP address at the base of the VPC IPv4 network range, with the last octet incremented by two digits. For example, the DNS Server on a 10.0.0.0/16 network is located at 10.0.0.2. For VPCs with multiple IPv4 CIDR blocks, the DNS server IP address is located in the primary CIDR block.

AWS HA uses several API requests to know the peer instance and also during IP switch-over. At the back-end, AWS has several servers with different IP address running to provide the SBC seamless performance or response. If one server goes down, the Amazon-provided DNS automatically updates the API endpoint. This may not be the case with the custom DNS and results in an API request failure. To overcome this issue, RAMP needs to add the field `AmazonProvidedDNS` in the DNS server, in addition to the IP address of the custom DNS server. For detailed information on the custom DNS, refer to [Using DNS with Your VPC](#) of the AWS documentation.

Create a Volume on AWS

Related articles:

- [Installing RAMP on AWS Manually](#)
- [Checklist for Installing RAMP on AWS](#)
- [Instantiate a Standalone RAMP Instance on AWS with Public IP Address](#)

Prior to launching a Ribbon Application Management Platform (RAMP) instance on Amazon Web Services (AWS), create an Elastic Block Store (EBS) storage volume for use by the instance. AWS provides a range of volume types and options, refer to the [Amazon EC2 User Guide for Linux Instances](#) for more information.

To create a volume on AWS, use the Amazon EC2 console. Refer to the [Amazon EC2 User Guide for Linux Instances](#) for the specific procedures. Ribbon recommends using the following values when creating a volume for a RAMP instance:

- **Volume type** – the recommended type is io1
- **Size** – the recommended size is 450Gb
- **Availability Zone** – as appropriate for the deployment and should be same as the RAMP instance
- **Snapshot ID** – is optional and not needed for RAMP.

After creating the volume, enter the volume ID that was generated for the volume when customizing the parameters in the CloudFormation template during the process of instantiating your RAMP instance.

Generate SSH Keys for RAMP Users on AWS

Related articles:

- [Installing RAMP on AWS Manually](#)
- [Checklist for Installing RAMP on AWS](#)
- [Instantiate a Standalone RAMP Instance on AWS with Public IP Address](#)

When you instantiate a Ribbon Application Management Platform (RAMP) instance on Amazon Web Services (AWS), the Cloud Formation template includes parameters to inject SSH public keys for the RAMP "admin" and "insight" users to enable password-less authentication.

Generate the SSH keys from a Linux server within the network in order to SSH from that Linux server, as the admin or insight user, without entering the password. You can perform SSH from any other server containing the SSH keys injected during the instantiation.

You can add additional SSH keys after the node instantiation using the `ssh-copy-id` tool. For more information, refer to [Establish Passwordless Connection from an External Server to RAMP](#).

To generate SSH keys:

1. Verify that the files `id_rsa` and `id_rsa.pub` exist on a Linux server and then enter the following command on the server:

```
ssh-keygen
```

The following message is displayed:

```
Generating public/private rsa key pair.
Enter file in which to save the key (<the home directory of the Linux
server>/.ssh/id_rsa):
```

2. Press **ENTER**:

The following message is displayed:

```
<the home directory of the Linux server>/.ssh/id_rsa already exists.
Overwrite (y/n)?
```

3. Enter **y**.

The following prompt is displayed:

```
Enter passphrase (empty for no passphrase):
```

4. Press **Enter**.

The following prompt is displayed:

```
Enter same passphrase again:
```

Example output:

```
Your identification has been saved in <the home directory of the Linux
server>/.ssh/id_rsa.
Your public key has been saved in <the home directory of the Linux server>/.ssh/
id_rsa.pub.
The key fingerprint is:
SHA256:NqYFcc0h0Jurdk6hBSQU+BCyV/UQwJBqNt3UUnQRf+I insight@treebeardVm3
The key's randomart image is:
+---[RSA 2048]-----+
| . oB*+@*o*+. |
| o+..= *o.+ |
| ..ooo + .o o . |
| .= ... oo . o |
| o . S. E |
| B.o |
| o.. |
| o.. |
| . o. |
+----[SHA256]-----+
```

Use the text in the file `<the home directory of the Linux server>/ssh/id_rsa.pub` as input in the AdminSshKey and InsightSshKey field when instantiating a RAMP instance. Refer to [Instantiate a Standalone RAMP Instance on AWS with Public IP Address](#).

Copy RAMP SSH Keys to an External Server

The SSH keys you generate for the RAMP insight user are needed when you instantiate PSX Primary instances and to restore RAMP instances. Copy the SSH keys to an external server so that they are backed up and available when needed.

To copy SSH keys from RAMP:

1. SSH to RAMP as the insight user:

```
ssh insight@<RAMP IP address>
```

2. Navigate to `.ssh`:

```
cd .ssh
```

3. List the files:

```
ls -l
```

Sample output appears below:

```
total 24
-rw----- 1 insight insight 1675 Oct 13 15:35 id_rsa
-rw-r--r-- 1 insight insight 409 Oct 13 15:35 id_rsa.pub
-rw-r--r-- 1 insight insight 4915 Oct 25 00:32 known_hosts
-rw-r--r-- 1 insight insight 4915 Oct 24 21:19 known_hosts.old
```

4. Obtain the public SSH key:

```
cat id_rsa.pub
```

Sample output of an SSH public key appears below:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCYpnuLMLZLJxgxvgkUdiy3SW5xL4uLLcpAQy2P6fdyrThWL0PiPH
8R0JjXn6PeYvcj69Qis0Hgb736RpoapaLpYcsA1qcHL07503174ImNsjr3c8b9uzea50Bt5dXgo4ChBZjw
9cKa4DCyqiqmeFvg3bot7q1LoVi/
cS43VFv+EPLL8fxQAZ2p8+6B2c0fsgREGTeAS11i9b2i456uC+fWvgiimMk8Zuzg9kCqkhneb7lHPmR/
KiDlhv5krXE0+P3g6co/01Mxi1bx7/8bprbTq6m71uOP4e6H+F9/fD++BmP/
dk7x1uB289Y6ZHtFXjdHRHLpk1CFmw7toyZ0Swj
insight@ramp-a310
```

Note

When you instantiate a PSX Primary node, enter the RAMP public SSH key in the "EmsSshKey1" field. This allows RAMP to access the PSX without a password.

5. Obtain the private SSH key:

```
cat /opt/sonus/ems/.ssh/id_rsa
```

Sample output of a SSH private key appears below:

```
-----BEGIN RSA PRIVATE KEY-----
MIIIEowIBAAKCAQEA3szwSndur3T72jJIDoKiMaIk0kuKdKMqADc0jtFvE8GWdYz
X2RS5qF1nLzfj4ui0cx/Cx/+EZMrJrnf/GH4nH6DRJaUtQglFo62NgPNZGgONADj
ThGLABjKLU07iDV5XeFPrZxzUSd72uPSEXK5w6f1uo9q06UbbAgSdPwnnk1ChKcS
GcbE7fNGe/wEtKYmsRw8ALe6FIzu9WRA0dbApLzLSZC5kV+PE7rC0f0qZiNjheZV
/lzbu0T3quAJD6reuSzEAzWJ9HhSLQa50X0GD+vyzRpAQnHi4EERZWV6zGndhTaI
rUyRqjMzFMdYnwE4aDJFs2RAYnwWTtYW4hH6QIDAQABaoIBACT3rESZCGtQcbK5
rN0ev0NkDhUxiRiBw9lbIZwyyC4u9LvUrR3qqrYL0xQLkWhJojr7rVK7pSbM8YA
aZShwJE3lYCiKC0Rg7rc60us3juCmZLHwZEPnDNior8n3D98v0rzlEn4xf7FR0Kz
Q96nlVp4wFY/eKheU/VFteQg9dHJUNGKmCw3tizBqXo7lIuP9paTDcWTWdta0Yf
rWVpY0968yrjx3PdJF06DHGgK9XeJ0CoRKMMzS8x0jhnWy/7ruRAYZtXvLdYT0Iu
nWcNFvgW0qFSz0ADCUMj51Pa47dLsAdyY1VjN8Ou3ZczNnPKizz9P7gP52jpw0dk
XrIL8AECgYEA+Rd6+USKEiKSUD+t00/jTcm0PYdBrEX3+raJawTa08u6NHE3QJnn
g0NvaLLIeNAihqUw6KlsKx1gCIFWJk278irwjiSp97+vMCGhXyp1s5eIROX60RjV
LWPjm49loJkVyqUs6LWkSmFrRGB1SPUtSKaVayQNCTfFRt6mVnaE8wECgYEA5PrL
Yhh21u/tqzb9iIAZgFrjt885f3ToUZjSXKEvFLUqa3sbzFhSrNREJAd80sgM2n2m
Yn5bUmJvzYVeFgbfDJeIIuLNj+brhSYdKdh5zB6nx4cmJm0zSaJiAYN2/cFuLtKx
1U9sHA8a9Zip+j+0vqSC+C1NvETtgqleJUjzH0kCgYBm2V8ZVVI5fWPmZqRsFQvp
roMRdKuVKj698mjCb7Y7BT+ZL7YUoneJJ2r02/0ShT38QnDzYCEdnD9uw5iCsE40
K9SvnEvh0+/N+9TZqnp28PZ/HEZ3170NNTSAl9/9DWf0pxUacuwOpFD5mAHA9Ty
znVwmo4XE08g2pDASTCAQKBgF8X7HkLsebnC2ukhbw3ft+4X1PJopZVJdolPk+r
vP3sevZyBQRjNcsvi9Durx8WZ4ghoITM9v4K1WWj2oQJTH5909NjH5eAjhUY1Am5
1jM4E/OgI+7XcPJG1q8M0tF9kFWvuJzEXAYPG+IdCZJc7NotlhqdLehfM8gMsIWJ
ezVpAoGBAKRx84JkNDNJ9SZtFSNxxDMzd/uRKbk9wntBF0sBNCrtqNsx/OCsZHye
CQ75MSxDL5NSOWtCK2Ln9fqAid/3rNsbwhFtMDKEEXnOoLLiN6wy9o/N8312VW4o
f/NTRELwvBssAovC7SWiTap67H5Mi/H9t8z/bFEPW6ptBYaxsQH
-----END RSA PRIVATE KEY-----
```

6. Perform one of the following to copy the keys to an external server:

- Transfer the *id_rsa* and *id_rsa.pub* files to an external server.
- Copy the output in Step 4 and Step 5 to a text file, and copy the text file to an external server.

Copy ssh Key to an External Server for RAMP PM Stats Export

1. Create a directory on the external server to store the exported statistics.

You can either create a new user or use an existing username on the external server.

- SSH to RAMP as insight user or login as admin and then switch to insight user.

```
ssh insight@<RAMP IP address>
```

- Copy RAMP's public (pub) key to external server as insight user.
For example,

```
ssh-copy-id -i <ssh username>@<externalServerIp>
```

- Now as insight user, log into the external server from RAMP. You should be able to login to the external server without being asked for a password.

```
ssh <ssh username>@<externalServer>
```

Checklist for Installing RAMP on AWS

During the Ribbon Application Management Platform (RAMP) instantiation process on Amazon Web Services (AWS), you provide parameter values that customize the CloudFormation template used to instantiate your deployment. The following table describes the parameters that are presented during the stack creation process. Review these parameters before you begin the instantiation process to collect mandatory values and determine which optional parameters you want to configure.

Field	Description	Mandatory?	Customizable by User?
Stack name	A unique name for the RAMP stack. A stack is a collection of AWS resources you create and delete as a single unit.	✓	✓
Network Configuration			
SubnetId	The subnet ID of an existing subnet in your virtual private cloud (VPC) that you want to use for the management interface.	✓	

Field	Description	Mandatory?	Customizable by User?
InstanceSecurityGroup	The security group to use to control both inbound and outbound traffic to the management interface and acts as a firewall for associated Amazon EC2 instances.	✓	
Amazon EC2 Configuration			
AmiId	The Amazon Machine Image (AMI) identifier. For example, <code>ami-xxxxxxx</code> . Refer to the RAMP release notes for the current value.	✓	
InstanceType	The type of instance to create. Refer to System Requirements .	✓	
MgmtPrivIP	The management IP address for the RAMP instance. If you do not specify a management IP, then one is automatically assigned. • MgmtPrivIP: is only for a private template. • RampPrivateIpAddress: is only for a public template. • RampPublicIpAddress: is only for a public template.		
Keyname	The name of an existing AWS EC2 key pair to enable SSH access to the RAMP instance for the RAMP admin user .	✓	
Volume Type	The type of Elastic Block Store (EBS) volume to use for RAMP. Example: <code>io1</code> <code>gp2</code> magnetic.	✓	
Iops	If the EBS volume type is <code>io1</code> , this value specifies the IOPS (input/output operations per second) reservation for the <code>io1</code> volume type.	✓	

Field	Description	Mandatory?	Customizable by User?
Volume ID	The volume ID for the volume to use for the RAMP instance. This is used for recovery if the RAMP instance goes down. For information refer to Create a Volume on AWS .	✓	
PlacementGroup	The name of an existing placement group. A placement group specifies the strategy you want to follow in deploying instances in your AWS environment. This is an optional field you can leave blank.		
RAMP Configuration			
Name	A name for the RAMP instance.	✓	✓
DnsServers	The DNS servers for the RAMP instance to use (comma delimited).		
NtpServers	The NTP servers for the RAMP instance to use (comma delimited). To use multiple NTP servers, enter the NTP server IP addresses in the following format: <pre>"<NTP server 1>","<NTP server 2>","<NTP server 3>"</pre> The following is an example: <pre>"10.1.1.6","10.128.254.67","10.128.254.68"</pre>	✓	
TimeZone	The time zone for the RAMP instance.		
RAMP Access Configuration			

Field	Description	Mandatory?	Customizable by User?
AdminSshKey	An SSH key generated on a Linux server to inject during instantiation to enable the admin user to access RAMP. To generate SSH key, refer to Generate SSH Keys for RAMP Users on AWS . Note that for RAMP geographically redundant (GR) deployments, the key for the source RAMP instance is included in the template for the target RAMP instance to enable setting up the GR connection between the instances.	✓	
InsightSshKey	An SSH key generated on a Linux server to inject during instantiation to enable the insight user to access RAMP. To generate SSH key, refer to Generate SSH Keys for RAMP Users on AWS .	✓	
RampPrivateIpAddress	You must leave this field blank for an install because the IP address is auto-assigned. For an upgrade, you must enter the private IP address of the older RAMP for reuse.		
RampPublicIpAddresses	Enter the previously created elastic IP address.	✓	

Instantiate a Standalone RAMP Instance on AWS with Public IP Address

The following procedure describes how to launch a Ribbon Application Management Platform (RAMP) instance using the Amazon Web Services (AWS) CloudFormation console. Before you begin, make sure you have completed the steps that prepare your environment that are outlined on [Installing RAMP on AWS Manually](#). Refer to [Amazon Cloud Formation documentation](#) for additional detailed documentation on working with stacks and using the CloudFormation console.

Note

Other Devices communicate with RAMP over the elastic IP address of RAMP. This is treated as the management IP address of RAMP. You must add the elastic IP address of devices into RAMP's security group to allow the devices to communicate with RAMP. Refer to [Create Security Groups and Security Group Rules on AWS](#)

Warning

- Do not update or modify the stack after creation.
- Do not change or remove resources after instance creation. For example, removing or attaching an elastic IP address, changing the user data, and so on.

Note About Deleting Instances

If you delete an instance, be aware that AWS does not delete volume(s) automatically. You must explicitly delete volumes you no longer want using the Amazon EC2 console. Refer to [Amazon Elastic Compute Cloud \(Amazon EC2\) documentation](#) for information.

To instantiate a RAMP standalone instance on AWS:

1. Open the AWS CloudFormation console.
2. Click **Create Stack - With new resources**.
The **Prerequisites - Prepare template** window opens.
3. Select **Template is ready** to specify to use the RAMP Cloud Formation template you downloaded from Ribbon.
4. Under **Specify template**, select **Upload a template file**.
5. Click **Choose file** and browse for the template file: `RAMP_AWS_CF_PUBLIC_TEMPLATE.yaml`.
6. Click **Next** to open the **Specify stack details** window.
7. Using the following table, edit the stack details to specify the parameters you want to use for the RAMP instance you are creating.

Field	Description	Mandatory?	Customizable by User?
Stack name	A unique name for the RAMP stack. A stack is a collection of AWS resources you create and delete as a single unit.	✓	✓
Network Configuration			
SubnetId	The subnet ID of an existing subnet in your virtual private cloud (VPC) that you want to use for the management interface.	✓	
InstanceSecurityGroup	The security group to use to control both inbound and outbound traffic to the management interface and acts as a firewall for associated Amazon EC2 instances.	✓	
Amazon EC2 Configuration			

Field	Description	Mandatory?	Customizable by User?
Amild	The Amazon Machine Image (AMI) identifier. For example, <code>ami-xxxxxx</code> . Refer to the RAMP release notes for the current value.	✓	
InstanceType	The type of instance to create. Refer to System Requirements .	✓	
Keyname	The name of an existing AWS EC2 key pair to enable SSH access to the RAMP instance for the RAMP admin user.	✓	
Volume Type	The type of Elastic Block Store (EBS) volume to use for RAMP. Example: <code>io1 gp2 magnetic</code> .	✓	
Iops	If the EBS volume type is <code>io1</code> , this value specifies the IOPS (input/output operations per second) reservation for the <code>io1</code> volume type.	✓	
Volume ID	The volume ID for the volume to use for the RAMP instance. This is used for recovery if the RAMP instance goes down. For information refer to Create a Volume on AWS .	✓	
PlacementGroup	The name of an existing placement group. A placement group specifies the strategy you want to follow in deploying instances in your AWS environment. This is an optional field and can be blank.		
RAMP Configuration			

Field	Description	Mandatory?	Customizable by User?
Name	A name for the RAMP instance. This name is used as the hostname for RAMP Note Re-use the same instance name in case of upgrade/migration.	✓	✓
DnsServers	The DNS servers for the RAMP instance to use (comma delimited).		
NtpServers	The NTP servers for the RAMP instance to use (comma delimited). To use multiple NTP servers, enter the NTP server IP addresses in the following format: "<NTP server 1>", "<NTP server 2>", "<NTP server 3>" The following is an example: "10.1.1.6", "10.128.254.67", "10.128.254.68"	✓	
TimeZone	The time zone for the RAMP instance.		
RAMP Access Configuration			

Field	Description	Mandatory?	Customizable by User?
AdminSshKey	An SSH key generated on a Linux server to inject during instantiation to enable the admin user to access RAMP. To generate SSH key, refer to Generate SSH Keys for RAMP Users on AWS . Note that for RAMP geographically redundant (GR) deployments, the key for the source RAMP instance is included in the template for the target RAMP instance to enable setting up the GR connection between the instances.	✓	
InsightSshKey	An SSH key generated on a Linux server to inject during instantiation to enable the insight user to access RAMP. To generate SSH key, refer to Generate SSH Keys for RAMP Users on AWS .	✓	
RampPrivateIpAddress	In case of an install, this needs to be blank, as the IP address is auto assigned. For an upgrade, you must enter the private IP address of the older RAMP for reuse.		
RampPublicIpAddress	Enter the previously created elastic IP address. To create an elastic IP address, refer to Allocate an Elastic IP Address .	✓	

8. Click **Next**. to open the **Configure stack options** window.
9. (Optional) Enter a **Key** and **Value** if you use tagging in your AWS environment. Refer to [AWS documentation](#) for information.

Note

Tagging key-value pairs to the stack is optional.

10. Click **Next** to open the **Review** window.
11. Review the stack details and click **Create**.
12. Once the stack creation starts, in the CloudFormation console, go to **Stack Details > Output > InstanceIpAddress**.
Information similar to the following appears.

Key	Value	Description	Export name
InstanceIPAddress	X.X.X.X	IP address of the newly created EC2 instance	-

Example stack parameter information:

Key	Value
AdminSshKey	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDrYRGdG5WEsdIXy Ko2hfwFMGb080+Oo9YITOGf+phT0p0VSKhTdgKwB2uiiD7Lc7C fZGZws/1q+kcy/6feHAPFvYdkySi8rSolhxNEFPwAYpGi/fsslp/ x5f4lF7zBbqemGVdZX/ 8IJGqHcN368dgm6k+b3/2leDFJjfw6zze7Yrf2M3uefU+ldSYjf0p5 7lzkAMsBuFETGyK4/ mrGV5sFP9aUZ3dinQ498zOZcAV+pL08XOOS1Tts7M7P0kxqVk DwtFtd87NwjYdYC9rM3tTqW7P8FPk6CQgvgMWvmUN1+m6fah 5uu6d21eJ2qnAVBtp9T5zOfVICsUcvNZv497p
AmiId	ami-0d4f77a0c1afa86cc
DnsServers	10.2.1.2
EnableCloudWatchMetrics	False
IAMRole	-
InsightSshKey	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDrYRGdG5WEsdIXy Ko2hfwFMGb080+Oo9YITOGf+phT0p0VSKhTdgKwB2uiiD7Lc7C fZGZws/1q+kcy/6feHAPFvYdkySi8rSolhxNEFPwAYpGi/fsslp/ x5f4lF7zBbqemGVdZX/ 8IJGqHcN368dgm6k+b3/2leDFJjfw6zze7Yrf2M3uefU+ldSYjf0p5 7lzkAMsBuFETGyK4/ mrGV5sFP9aUZ3dinQ498zOZcAV+pL08XOOS1Tts7M7P0kxqVk DwtFtd87NwjYdYC9rM3tTqW7P8FPk6CQgvgMWvmUN1+m6fah 5uu6d21eJ2qnAVBtp9T5zOfVICsUcvNZv497p
InstanceSecurityGroup	sg-07006b2e8b7d760f6
InstanceType	m5.4xlarge
Iops	1000
KeyName	EMS_SVT

Key	Value
Name	rampInstance
NtpServers	10.1.1.6
PlacementGroup	-
RAMPPrivatelPAddress	-
RAMPPublicIpAddress	184.72.222.234
SubnetId	subnet-0452dfb93fb2e453e
TimeZone	America/NewYork
Volumeld	vol-02c8ed983f7d62607

The EIP used for RAMP will be auto assigned to RAMP's security group (inbound/outbound rules). For more information on security groups, refer to [Create Security Groups and Security Group Rules on AWS](#). Once the stack is successfully created, the instance is added to the stack list.

The RAMP's localhost node is registered with the elastic IP address of RAMP.

Instantiate a Standalone RAMP Instance on AWS with Private IP Address

Use the following procedure to launch a Ribbon Application Management Platform (RAMP) instance using the Amazon Web Services (AWS) CloudFormation console. Before you begin, make sure you have completed the steps that prepare your environment that are outlined on [Installing RAMP on AWS Manually](#). Refer to [Amazon Cloud Formation documentation](#) for additional detailed documentation on working with stacks and using the CloudFormation console.

Warning

- Do not update or modify the stack after creating it.
- Do not change or remove resources after instance creation (For example, removing or attaching an elastic IP, changing the user data, and so on).

Note About Deleting Instances

If you delete an instance, be aware that AWS does not delete volume(s) automatically. You must explicitly delete volumes you no longer want, using the Amazon EC2 console. Refer to [Amazon Elastic Compute Cloud \(Amazon EC2\) documentation](#) for information.

To instantiate a RAMP standalone instance on AWS:

1. Open the AWS CloudFormation console.
2. Click **Create Stack - With new resources**.
The **Prerequisites - Prepare template** window opens.
3. Select **Template is ready** to specify to use the RAMP Cloud Formation template you downloaded from Ribbon.
4. Under **Specify template**, select **Upload a template file**.
5. Click **Choose file** and browse for the template file: `RAMP_AWS_CF_PRIVATE_TEMPLATE.yml`.
6. Click **Next** to open the **Specify stack details** window.
7. Using the following table, edit the stack details to specify the parameters you want to use for the RAMP instance you are creating.

Field	Description	Mandatory?	Customizable by User?
Stack name	A unique name for the RAMP stack. A stack is a collection of AWS resources you create and delete as a single unit.	✓	✓
Network Configuration			
SubnetId	The subnet ID of an existing subnet in your virtual private cloud (VPC) that you want to use for the management interface.	✓	
InstanceSecurityGroup	The security group to use to control both inbound and outbound traffic to the management interface and acts as a firewall for associated Amazon EC2 instances.	✓	
Amazon EC2 Configuration			
AmiId	The Amazon Machine Image (AMI) identifier. For example, <code>ami-xxxxx</code> . Refer to the RAMP release notes for the current value.	✓	
InstanceType	The type of instance to create. Refer to System Requirements .	✓	

Field	Description	Mandatory?	Customizable by User?
MgmtPrivIP	The management IP address for the RAMP instance. If you do not specify a management IP, then one is automatically assigned. Note In case of Migration or upgrade, this field is mandatory.		
Keyname	The name of an existing AWS EC2 key pair to enable SSH access to the RAMP instance for the RAMP admin user.	✓	
Volume Type	The type of Elastic Block Store (EBS) volume to use for RAMP. Example: io1 gp2 magnetic.	✓	
Iops	If the EBS volume type is io1, this value specifies the IOPS (input/output operations per second) reservation for the io1 volume type.	✓	
Volume ID	The volume ID for the volume to use for the RAMP instance. This is used for recovery if the RAMP instance goes down. For information refer to Create a Volume on AWS .	✓	
PlacementGroup	The name of an existing placement group. A placement group specifies the strategy you want to follow in deploying instances in your AWS environment. This is an optional field and can be blank.		
RAMP Configuration			

Field	Description	Mandatory?	Customizable by User?
Name	A name for the RAMP instance. This name is used as the hostname for RAMP. Re-use the same instance name in case of upgrade/migration.	✓	✓
DnsServers	The DNS servers for the RAMP instance to use (comma delimited).		
NtpServers	The NTP servers for the RAMP instance to use (comma delimited). To use multiple NTP servers, enter the NTP server IP addresses in the following format: "<NTP server 1>", "<NTP server 2>", "<NTP server 3>" The following is an example: "10.1.1.6", "10.128.254.67", "10.128.254.68"	✓	
TimeZone	The time zone for the RAMP instance.		
RAMP Access Configuration			
AdminSshKey	An SSH key generated on a Linux server to inject during instantiation to enable the admin user to access RAMP. To generate SSH key, refer to Generate SSH Keys for RAMP Users on AWS. Note that for RAMP geographically redundant (GR) deployments, the key for the source RAMP instance is included in the template for the target RAMP instance to enable setting up the GR connection between the instances.	✓	

Field	Description	Mandatory?	Customizable by User?
InsightSshKey	An SSH key generated on a Linux server to inject during instantiation to enable the insight user to access RAMP. To generate SSH key, refer to Generate SSH Keys for RAMP Users on AWS .	✓	

8. Click **Next** to open the **Configure stack options** window.
9. (Optional) Enter a **Key** and **Value** if you use tagging in your AWS environment. Refer to [AWS documentation](#) for information.

Note

Tagging key-value pairs to the stack is optional.

10. Click **Next** to open the **Review** window.
11. Review the stack details and click **Create**.
12. Once the stack creation starts, in the CloudFormation console, go to **Stack Details > Output > InstanceIPAddress**.

Information similar to the following appears.

Key	Value	Description	Export name
InstanceIPAddress	X.X.X.X	IP address of the newly created EC2 instance	-

Example stack parameter information:

Key	Value
AdminSshKey	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDrYRGdG5WEsdIXy Ko2hfwFMGb080+Oo9YITOGf+phT0p0VSKhTdgKwB2uiiD7Lc7C fZGZws/1q+kcy/6feHAPFvYdkySi8rSolhxNEFPwAYpGi/fsslp/ x5f4IF7zBbqemGVdZX/ 8IJGqHcN368dgm6k+b3/2leDFJjfw6zze7Yrf2M3uefU+ldSYjf0p5 7lzkAMsBuFETGyK4/ mrGV5sFP9aUZ3dinQ498zOZcAV+pL08XOOS1Tts7M7P0kxqVk DwtFtd87NwjYdYC9rM3tTqW7P8FPk6CQgvgMWvmUN1+m6fah 5uu6d21eJ2qnAVBtp9T5zOfVICsUcvNZv497p
Amild	ami-04642ac93ee6896c7
DnsServers	10.2.1.2
EnableCloudWatchMetrics	False

Key	Value
IAMRole	-
InsightSshKey	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDrYRGdG5WEsdIXy Ko2hfwFMGb080+Oo9YITOGf+phT0p0VSKhTdgKwB2uiiD7Lc7C fZGZws/1q+kcy/6feHAPFvYdkySi8rSolhxNEFPwAYpGi/fsslp/ x5f4lF7zBbqemGVdZX/ 8lJGqHcN368dgm6k+b3/2leDFJjfw6zze7Yrf2M3uefU+ldSYjf0p5 7lzkAMsBuFETGyK4/ mrGV5sFP9aUZ3dinQ498zOZcAV+pL08XOOS1Tts7M7P0kxqVk DwtFtd87NwjYdYC9rM3tTqW7P8FPk6CQgvgMWvmUN1+m6fah 5uu6d21eJ2qnAVBtp9T5zOfVICsUcvNZv497p
InstanceSecurityGroup	sg-07006b2e8b7d760f6
InstanceType	m5.4xlarge
Iops	1000
KeyName	EMS_SVT
ManagementPrivateIP	-
Name	rampinstance
NtpServers	10.1.1.6
PlacementGroup	-
SubnetId	subnet-0452dfb93fb2e453e
TimeZone	America/New_York
VolumeId	vol-0ec647cac82ef5701
VolumeType	gp2

Once the stack is successfully created, the instance is added to the stack list.

Allocate an Elastic IP Address

Ribbon Access Management (RAMP) supports elastic IP addresses. If you selected RAMP_AWS_CF_PUBLIC template, then perform the following procedure to allocate an elastic IP address to your account. The RAMP

instance created is associated with both the private IP and Elastic IP (EIP) addresses. A private IP address is only reachable within the same Virtual Private Cloud (VPC) or across different VPCs with peering, whereas an EIP is accessible across the internet.

Here are few characteristics of an EIP:

- An EIP address is static and does not change over time.
- An EIP address is used in a specific region only – you cannot move it to a different region.
- An EIP address comes from Amazon's pool of IPv4 addresses or from a custom IPv4 address pool that you brought to your AWS account.
- To use an EIP address, you first allocate one to your account and associate it with your instance or a network interface.
- When you associate an EIP address with an instance, it is also associated with the instance's primary network interface. When you associate an EIP address with a network interface that is attached to an instance, it is also associated with the instance.

Prerequisites

- Login credentials for your AWS account.

Start

1. Log onto your AWS account.
2. Navigate to **EC2 > Network & Security > Elastic IPs**.
3. Click **Allocate Elastic IP Address**.
4. In the **Network Border Group**, select the region where you want to bring up the instance.

For example:

Network Border Group	Us-east-1

5. From the **Public IPv4 address** pool, select the Amazon's pool of IPv4 addresses.

Public IPv4 address	Amazon's pool of IPv4 addresses

6. Click **Allocate**.
7. Use this elastic IP address while creating the RAMP stack.

Installing RAMP on Azure Manually

You can manually install Ribbon Application Management Platform (RAMP) in a Microsoft Azure cloud environment using the procedures outlined in this topic.

Note

Cross-platform support is not available for Azure. You cannot register devices brought up on other platforms (for example, AWS) to RAMP on Azure.

The workflow below provides an overview of the process and provides links to the specific information and steps required to complete installation. After completing the steps on a linked page, return to the workflow for the next procedure.

Step	Action	Procedure
1	Ensure you have a current Microsoft Azure account and subscription.	
2	Contact Ribbon Support to obtain access to the RAMP image file in Azure.	
3	Review System Requirements to ensure your environment has the necessary resources and prerequisite software available.	System Requirements
4	Download the <code>CreateUIDefinition.json</code> file and RAMP template file from the Ribbon Support Portal. Select the file based on your requirements. • RAMP with a private IP – Download <code>RAMP_AZURE_CF_PRIVATE_TEMPLATE</code> The private IP is employed when the Virtual Network gateway for VPN is accessible within the On-prem lab, and ExpressRoute is set up on their On-prem network. • RAMP with a public IP – Download <code>RAMP_AZURE_CF_PUBLIC_TEMPLATE</code> The RAMP possesses a public IP address along with a private IP address, making it usable when RAMP needs to be accessible over the Internet.	Download Files from Ribbon Support Portal
5	Upload the RAMP template file to Azure.	Upload the RAMP Template to Azure
6	Create a resource group for RAMP resources.	Create a Resource Group for RAMP on Azure
7	Create a network security group for RAMP.	Create a Network Security Group for RAMP on Azure
8	Create an external disk for RAMP.	Create an External Disk for RAMP on Azure

Step	Action	Procedure
9	Generate SSH keys to inject for the RAMP insight and admin users to enable password-less access.	Generate SSH Keys for RAMP Users on Azure
10	Review the Checklist for Installing RAMP on Azure to ensure you have the parameter values you will need to update the template file for your deployment.	Checklist for Installing RAMP on Azure
11	Choose the parameters in the CreateUIDefinition.json file.	Generate Output Payload from createUIDefinition Sandbox
12	Complete Instantiate a Standalone RAMP Instance on Azure to create a standalone instance of RAMP.	Instantiate a Standalone RAMP Instance on Azure
13	(Optional) If you plan to manage SBC Edge devices with RAMP, enable the EdgeView (EV) service.	Deploy Optional Services on RAMP
14	Install RAMP licenses.	License Management

After completing installation, refer to the RAMP [RAMP User Guide](#) for additional information on configuring and working with RAMP.

Upload the RAMP Template to Azure

Related articles:

- [Installing RAMP on Azure Manually](#)
- [Checklist for Installing RAMP on Azure](#)
- [Instantiate a Standalone RAMP Instance on Azure](#)

Complete the following procedure to upload the **Ribbon Application Management Platform (RAMP)** template file to the Microsoft Azure Portal. The RAMP template is required to instantiate a RAMP instance on Azure.

Prerequisite

Obtain the RAMP template file from the Ribbon Support Portal. Refer to [Download Files from Ribbon Support Portal](#) for more information.

1. Open the RAMP template file in an editor and copy the entire contents of the file to your browser clipboard.
2. Access the Microsoft Azure Portal.
3. Go to the **Templates** page by clicking the **Templates** icon or by using the search bar.
4. Click **create** to open the **Add template** window with the **General** tab open.
5. In **Name**, enter a name for the template.
6. In **Description**, enter a description for the template.

7. Click **ARM Template** to open the **ARM Template** tab.
8. Replace any default contents that appear in the window with the contents of the RAMP template file you copied to the clipboard.
9. Click **Add** to save the contents as a template file on Azure.

Create a Resource Group for RAMP on Azure

Related articles:

- [Installing RAMP on Azure Manually](#)
- [Checklist for Installing RAMP on Azure](#)
- [Instantiate a Standalone RAMP Instance on Azure](#)

Complete the following procedure within the Microsoft Azure Portal to create a resource group for **Ribbon Application Management Platform (RAMP)**. A resource group in Azure is similar to a folder and is used to organize and manage resources. You create the resource group within your subscription.

1. Access the Microsoft Azure Portal.
2. Go to the **Resources group** page by clicking the **Resources group** icon or by using the search bar.
3. Click **create**.
4. In **Subscription**, select your subscription.
5. In **Resource group**, enter a name for the new resource group.
6. In **Region**, select the Azure region in which to create the resource group.
7. Click **review+create**.
8. Verify that the parameter values are correct and click **Create** to add the resource group.
9. Include the newly created resource group to a user group. See [Add User Groups](#).

Create a Network Security Group for RAMP on Azure

Related articles:

- [Installing RAMP on Azure Manually](#)
- [Checklist for Installing RAMP on Azure](#)
- [Instantiate a Standalone RAMP Instance on Azure](#)

Complete the following procedure within the Microsoft Azure Portal to create a network security group for **Ribbon Application Management Platform (RAMP)**. The network security group contains the security rules that permit inbound and outbound access to RAMP.

1. Access the Microsoft Azure Portal.
2. Go to the **Network security group** page by clicking the **Network security group** icon or by using the search bar.

3. Click **create**.
4. In **Subscription**, select your subscription.
5. In **Resource group**, select the name of the resource group for RAMP.
6. In **Name**, enter a name for the network security group.
7. In **Region**, select the Azure region in which to create the new network security group.
8. Click **review+create**.
9. Verify that the parameter values are correct and click **Create** to add the network security group.
When initially created, the network security group does not contain any rules permitting access to RAMP.
As you complete the RAMP instantiation procedure, you must add rules for your specific deployment.
Refer to [Instantiate a Standalone RAMP Instance on Azure](#).

Inbound Security Group Rule Port Descriptions

Ribbon recommends to open the following ports using Inbound/Ingress rules in the security groups associated with the management interface.

For a complete list of RAMP ports, refer to [RAMP Ports Descriptions](#).

Inbound Ports

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Management IP of devices	Secure login to RAMP from a console terminal through SSH.
Custom UDP Rule	UDP	123	Management IP of devices	Network Time Protocol for clock synchronization. This is optional and only required when using an external NTP server.
Custom UDP Rule	UDP	161	Management IP of devices	SNMP reachability polling for the RAMP node.
Custom UDP Rule	UDP	162	Management IP of devices	SNMP Event notification V2 trap from other devices to RAMP.
HTTPS	TCP	443	Management IP of devices	Redirects requests to JBoss application server, the RAMP Web GUI, SOAP and REST APIs.

Type	Protocol	Port Range	Source	Description
Custom UDP Rule	UDP	5200	Management IP of devices	Agent trap receiver port used for receiving hardware traps sent from port 1610.
Custom TCP Rule	TCP	5432	Management IP of devices	PostgreSQL database – internal DB connections.
Custom TCP Rule	TCP	6462	Management IP of devices	Used for enabling FTP statistics collection from RAMP.
Custom TCP Rule	TCP	8122	Management IP of devices	Remote access to the RAMP CLI from a client through SSH.
Custom TCP Rule	TCP	9001	Management IP of devices	Client/server communication from PSX Manager to RAMPt through a PSX proxy server over HTTPS (SSL).
Custom UDP Rule	UDP	9004	Management IP of devices	Call Trace event notification from other devices to RAMP.
All ICMP - IPv4	All	N/A	Management IP of devices	
All traffic	All	All	Public management IP of RAMP	This is required only when RAMP is instantiated with public IP address.

Outbound Ports

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Management IP of devices	Connection (Tunneled protocols such as PIPE and so on).
Custom UDP Rule	UDP	123	Management IP of devices	Network Time Protocol for clock synchronization.
Custom UDP Rule	UDP	161	Management IP of devices	SNMP reachability polling for the RAMP node.
Custom UDP Rule	UDP	162	Management IP of devices	SNMP event notification V2 trap from other devices to RAMP.

Type	Protocol	Port Range	Source	Description
HTTPS	TCP	443	Management IP of devices	RAMP GUI access.
Custom TCP Rule	TCP	444	Management IP of devices	SBC platform port, used for inventory collection.
Custom UDP Rule	UDP	514	Management IP of devices	syslogd.
Custom UDP Rule	UDP	1812	Management IP of devices	Radius authentication port (configurable - this is the default).
Custom TCP Rule	TCP	2022	Management IP of devices	NETCONF sessions to SBCs.
Custom TCP Rule	TCP	2024	Management IP of devices	SFTP to SBC.
Custom TCP Rule	TCP	6462	Management IP of devices	RAMP and PSX communication (SFTP stats collection) using REST.
Custom TCP Rule	TCP	19991	Management IP of devices	Sonus agent configuration
All ICMP - IPv4	All	N/A	Management IP of devices	
All traffic	All	All	Public management IP of RAMP	This is required only when RAMP is instantiated with public IP address.

Create an External Disk for RAMP on Azure

Related articles:

- [Installing RAMP on Azure Manually](#)
- [Checklist for Installing RAMP on Azure](#)
- [Instantiate a Standalone RAMP Instance on Azure](#)

Complete the following procedure within the Microsoft Azure Portal to create an external disk to attach to the Ribbon Application Management Platform (RAMP) instance.

1. Access the Microsoft Azure Portal.
2. Go to the **Disks** page by clicking the **Disks** icon or by using the search bar.
3. Click **create**.
4. In **Subscription**, select your subscription.
5. In **Resource group**, select the resource group for RAMP.
6. In **Disk name**, enter a name for the new disk.
7. In **Region**, select the Azure region in which to create the disk.
8. In **Disk size**, select either a Premium SSD LRS or a standard HDD disk that is 450 GB in size. If the size specified is not 450 GB, click the **Change size** link to open a window where you can specify a size of 450 GB for the disk.
9. Click **review+create**.
10. Verify that the parameter values are correct and click **Create** to create the disk.

Generate SSH Keys for RAMP Users on Azure

Related articles:

- [Installing RAMP on Azure Manually](#)
- [Checklist for Installing RAMP on Azure](#)
- [Instantiate a Standalone RAMP Instance on Azure](#)

When you instantiate a Ribbon Application Management Platform (RAMP) instance on Microsoft Azure, the template includes parameters to inject SSH public keys for the RAMP "admin" and "insight" users to enable password-less authentication.

Generate the SSH keys from a Linux server within the network in order to SSH from that Linux server, as the admin or insight user, without entering the password. You can perform SSH from any other server containing the SSH keys injected during the instantiation.

You can add additional SSH keys after the node instantiation using the `ssh-copy-id` tool. For more information, refer to [Establish Passwordless Connection from an External Server to RAMP](#).

To generate SSH keys:

1. Verify that the files `id_rsa` and `id_rsa.pub` exist on a Linux server and then enter the following command on the server:

```
ssh-keygen
```

The following message is displayed:

```
Generating public/private rsa key pair.
```

```
Enter file in which to save the key (<the home directory of the Linux
server>/.ssh/id_rsa):
```

2. Press **ENTER**:
The following message is displayed:

```
<the home directory of the Linux server>/.ssh/id_rsa already exists.
Overwrite (y/n)?
```

3. Enter **y**.
The following prompt is displayed:

```
Enter passphrase (empty for no passphrase):
```

4. Press **Enter**.
The following prompt is displayed:

```
Enter same passphrase again:
```

Example output:

```
Your identification has been saved in <the home directory of the Linux
server>/.ssh/id_rsa.
Your public key has been saved in <the home directory of the Linux server>/.ssh/
id_rsa.pub.
The key fingerprint is:
SHA256:NqYFcc0h0Jurdk6hBSQU+BCyV/UQwJBqNt3UUnQRf+I insight@treebeardVm3
The key's randomart image is:
+---[RSA 2048]-----+
| . oB*+@*o*+.      |
| o+..= *o.+        |
| ..ooo + .o o .    |
| .= ... oo . o     |
| o .      S. E      |
|      B.o          |
|      o..          |
|      o..          |
|      . o.         |
+-----[SHA256]-----+
```

Use the text in the file `<the home directory of the Linux server>/.ssh/id_rsa.pub` as input in the Admin Public Key and Insight Public Key fields when you instantiate a RAMP instance. Refer to [Instantiate a Standalone RAMP Instance on Azure](#).

Checklist for Installing RAMP on Azure

Related articles:

- [Installing RAMP on Azure Manually](#)
- [Instantiate a Standalone RAMP Instance on Azure](#)

During the Ribbon Application Management Platform (RAMP) instantiation process on Microsoft Azure, you provide parameter values that customize the template used to instantiate your deployment. The following table describes the parameters that you must select or provide. Review these parameters before you begin the instantiation process to collect mandatory values and determine which optional parameters you want to configure.

Field	Description	Mandatory?
Basics – Project details		
Subscription Resource Group	Select your Azure subscription and the resource group in which to create the virtual machine (VM) for the RAMP instance. Refer to Create a Resource Group for RAMP on Azure .	✓
Basics – Instance details		
Region	Select the region where you want to create the VM. Ribbon recommends selecting the region closest to the voice end user. If you plan to reuse an existing resource, select the region for the resource.	✓
Virtual Machine Name	Enter a name for the VM.	✓
Virtual Machine Settings – Azure VM size		
Virtual Machine Size	Select the VM size. The default is 1xStandard D16s v3, which includes 16 vcpus and 64 GB of memory.	✓
Image	Select the RAMP image file from the list. The image file must be present in a resource group within your subscription to appear in the list. To obtain access to the image file on Azure, contact Ribbon Support.	✓
Network Settings – Configure virtual networks		

Field	Description	Mandatory?
RAMP virtual network	Select an existing vnet, or create a new one, to act as a virtual private network that allows resources to communicate with each other securely. To create a new network when you are editing the RAMP template: 1. Click the Create new link to open a Create virtual network pane where you can provide a name for the network. 2. Click OK. The name of the new network appears as the RAMP virtual network and a new subnet is added. For more information, refer to Create a New or Select an Existing Resource for Virtual Network.	✓
Subnet	The subnet defines a particular range of IP addresses that will contain the RAMPprivate IP address. A subnet is also created when creating a new virtual network.	✓
Network Security Group	Select the name of the network security group you created for RAMP. This will contain the inbound and outbound access rules for RAMP. Refer to Create a Network Security Group for RAMP on Azure .	✓
RAMP Configuration Settings – RAMP Configuration User Interface		
Admin Public Key	An SSH key generated on a Linux server to inject during instantiation to enable the admin user to access RAMP from that server without a password. To generate SSH key, refer to Generate SSH Keys for RAMP Users on Azure .	✓
Insight Public Key	An SSH key generated on a Linux server to inject during instantiation to enable the insight user to access RAMP from that server without a password. To generate SSH key, refer to Generate SSH Keys for RAMP Users on Azure .	✓
RAMP Configuration Settings – RAMP System Identifiers		
DNS Host Name	The DNS server for the RAMP instance to use.	
NTP Server	The NTP server for the RAMP instance to use.	
Time Zone	The time zone for the RAMP instance.	

Field	Description	Mandatory?
External Disk	Select the external disk you created to associate with the RAMP instance. Refer to Create an External Disk for RAMP on Azure .	✓

Instantiate a Standalone RAMP Instance on Azure

Related articles:

- [Installing RAMP on Azure Manually](#)
- [Checklist for Installing RAMP on Azure](#)
- [Create a Public IP Address](#)

Use the following procedure to launch a Ribbon Application Management Platform (RAMP) instance using the Microsoft Azure Portal. Before you begin, ensure you have completed the steps that prepare your environment at [Checklist for Installing RAMP on Azure](#):

Note

By default, all the resources are created in the RAMP resource group. If you need different resource groups for the Network Security Group and Virtual Networks, then make the resources first and then use them as "existing" resources while creating RAMP.

Note

For public template:

- For an existing Virtual Network or subnet, manually add the RAMP IP address to the Network Security Group.
- For a new Virtual Network, the RAMP IP address is automatically associated with the Network Security Group.

To instantiate a RAMP standalone instance on Microsoft Azure:

1. From the Azure Home page, navigate to the **Templates** window (**Home > Templates**).
2. Select the RAMP template from the list.
3. Click **Deploy**.
4. Click **Edit parameters** at the top of the page to open the template in JSON format. For more information, refer to the [Checklist for Installing RAMP on Azure](#).
5. Copy the output payload to the **Edit parameters** page.
Here is a sample table:

Parameter	Sample value
BASICS	
Description	Ribbon
Resource Group	<enter your resource group>
Location	(US) East US.
SETTINGS	
Project Name	Ribbon-RAMP-SA
Location	eastus

Parameter	Sample value
Virtual Network	<pre>{ "name": "RAMP_RESOURCE_GROUP", "resourceGroup": "RAMP_RESOURCE_GROUP", "addressPrefixes": ["10.0.0.0/16"], "addressPrefix": "10.0.0.0/16", "newOrExisting": "existing", "subnets": { "subnet1": { "name": "subnet1", "addressPrefix": "10.0.0.0/24", "startAddress": "10.0.0.4" } } }</pre> Note For more information on the option: "newOrExisting": "existing", refer to Create a New or Select an Existing Resource for Virtual Network.
Public IP Address Name	(Only valid for a public template) You can leave This optional parameter blank while installing or upgrading RAMP. If this field is left blank, the system creates a public IP address automatically. Update this field if you want to use an existing public IP address during installation. Provide the Public IP Address Name. For more information, refer to Create a Public IP Address. Note Ensure the existing Public IP Address is in the same resource group as RAMP.

Parameter	Sample value
Network Security Group	/subscriptions/8b9b06b1-a850-4ddf-b008-17bc9cbc1d05/resourceGroups/ RAMP_RESOURCE_GROUP/providers/Microsoft.Network/networkSecurityGroups/ ramp_network_security_group
Management Private IP	(Only valid for private template) You must leave this field blank when installing a new RAMP. During the upgrade, provide the private IP address of the older RAMP you are re-using, as applicable.
Admin Ssh Key	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDrYRGdG5WEsdLXyKo2hfwFMGb080+0o9YlTOGf+p hT0p0VSKhTdGKwB2uiiD7Lc7CfZGZws/1q+kcy/ 6feHAPFvYdkySi8rSoIhxNEFPwAYpGi/fsslp/ x5f4lF7zBbqemGVdZX/ 8IJGqHcN368dgm6k+b3/2IeDFJj fjw6zze7Yrf2M3uefU+ldSYj f0p57IzkAMsBuFETGyK 4/mrGV5sFP9aUZ3dinQ498z0ZcAV+pL08X00S1Tts7M7P0kxqVkDwtFtd87NwjYdYC9rM 3tTqW7P8FPk6CQgvgMWvmUN1+m6fah5uu6d21eJ2qnAVBtp9T5z0fVICsUcvNZv497p siagarwal@bats19
Insight Ssh Key	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDrYRGdG5WEsdLXyKo2hfwFMGb080+0o9YlTOGf+p hT0p0VSKhTdGKwB2uiiD7Lc7CfZGZws/ 1q+kcy/6feHAPFvYdkySi8rSoIhxNEFPwAYpGi/fsslp/x5f4lF7zBbqemGVdZX/ 8IJGqHcN368dgm6k+b3/2IeDFJj fjw6zze7Yrf2M3uefU+ldSYj f0p57IzkAMsBuFETGyK 4/mrGV5sFP9aUZ3dinQ498z0ZcAV+ pL08X00S1Tts7M7P0kxqVkDwtFtd87NwjYdYC9rM3tTqW7P8FPk6CQgvgMWvmUN1+m6fah 5uu6d21eJ2qnAVBtp9T5z0fVICsUcvNZv497p siagarwal@bats19

Parameter	Sample value
Volume Id	/subscriptions/572e564f-87ea-4269-aadb-a14739637a31/resourceGroups/RBBN-SBC-DEV1/providers/Microsoft.Compute/disks/stiwari-sipp1_disk1_9b55b94e1c964ff7b04ab5e678172e59
Volume Name	stiware-sipp1_disk1_9b55b94e1c964ff7b04ab5e678172e59
Dns Servers	10.2.1.2
Ntp Servers	"10.1.1.6"
TimeZone	America/New_York

Parameter	Sample value																		
Network interface	◦ No NIC name provided: A new Network Interface is created with name as projectName-nic which has the above configured Virtual Network and Network Security Group attached to it. ◦ Provide new NIC name: Enter the following parameters to create a new Network Interface by navigating to Home > Network Interfaces > Create network interface. <table> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td>Subscription</td><td>Subscription name.</td></tr> <tr> <td>Resource group</td><td>Specify the Resource group name on which the RAMP would be created.</td></tr> <tr> <td>Name</td><td>Name of the NIC. For example: <i>rbbn-nic</i>.</td></tr> <tr> <td>Region</td><td>Specify the region on which the RAMP would be created.</td></tr> <tr> <td>Virtual network</td><td>Specify the Virtual network name that is already created and associated with a Security group.</td></tr> <tr> <td>Subnet</td><td>Specify the already created subnet name under the Virtual network.</td></tr> <tr> <td>IP version</td><td>Select IPv4 (No IPv6 support for RAMP on Azure).</td></tr> <tr> <td>Private IP address assignment</td><td>Select Static.</td></tr> </table> ◦ Provide existing NIC name:- Ensure that the NIC name specified here is associated with the same Virtual Network and Network Security Group values defined above. Else, it will be overwritten with the above-defined values.	Parameter	Description	Subscription	Subscription name.	Resource group	Specify the Resource group name on which the RAMP would be created.	Name	Name of the NIC. For example: <i>rbbn-nic</i> .	Region	Specify the region on which the RAMP would be created.	Virtual network	Specify the Virtual network name that is already created and associated with a Security group .	Subnet	Specify the already created subnet name under the Virtual network.	IP version	Select IPv4 (No IPv6 support for RAMP on Azure).	Private IP address assignment	Select Static .
Parameter	Description																		
Subscription	Subscription name.																		
Resource group	Specify the Resource group name on which the RAMP would be created.																		
Name	Name of the NIC. For example: <i>rbbn-nic</i> .																		
Region	Specify the region on which the RAMP would be created.																		
Virtual network	Specify the Virtual network name that is already created and associated with a Security group .																		
Subnet	Specify the already created subnet name under the Virtual network.																		
IP version	Select IPv4 (No IPv6 support for RAMP on Azure).																		
Private IP address assignment	Select Static .																		

- Click **Save**.
- Review the template data shown and then check the box that indicates you agree to the terms and conditions.
- Click **Purchase**.
- After receiving the "Validation Passed" message, click **Create** to deploy RAMP.
- Once the instantiation completes, navigate to **All services > Virtual machines** and select the new RAMP instance.
If you have selected an existing virtual network, add the public IP of RAMP to security group rules inbound/outbound. For more information, refer to [Create a New or Select an Existing Resource for Virtual Network](#).
- Use the public IP address to begin accessing the new RAMP instance.

Create a New or Select an Existing Resource for Virtual Network

Use the table on this page to differentiate between selecting an existing resource and creating a new resource for a Virtual Network (VNet) on the Ribbon Application Management Platform (RAMP).

Select an Existing Resource for a Virtual Network	Create a New Resource for a Virtual Network
Manually associate the Network Security Group (NSG) to the subnet of the VNet.	The NSG and the VNet are automatically associated during deployment.
The existing rules of the NSG are not modified and remains the same as earlier. You must manually add the RAMP IP address to the NSG.	The existing rules of the associated NSG get flushed. The RAMP IP address is automatically added to the NSG.
You may choose any VNet and NSG from any resource group.	The VNet and NSG are always created in the same resource group as the instance. For example, If the instance is created in resource group "A": • If you select an existing NSG within the same resource group "A", the NSG is reset by flushing all the rules and adding a RAMP IP address. • If you select the NSG from a resource group other than "A", a new NSG is created with the same name in the resource group "A".

Create a Public IP Address

Use the following procedure to create a public IP address for an instance of the Ribbon Application Management Platform (RAMP) using the Microsoft Azure portal. Before you begin, make sure you have completed the steps that prepare your environment at [Checklist for Installing RAMP on Azure](#).

To create a public IP address:

Start

1. From the Azure Home page, click the icon for **Public IP Address** or search for Public IP Address using the search bar to access the Public IP Address window.
2. Click **Create**.
3. Use the following table to update the parameters:

Parameters to Create a Public IP Address

Parameter	Description	Length/Range
Subscription	Select your subscription.	
Resource group	Select the resource group for RAMP.	

Parameter	Description	Length/Range
Instance Details		
Region	Select the Azure region to create the public IP address. Note This should be in the same region as that of the resource group.	
Configuration Details		
Name	Enter a name for the new public IP address.	
IP Version	Select IPv4: ◦ IPv4 ◦ IPv6 The default value is "IPv4".	
SKU	Select Standard: ◦ Standard ◦ Basic The default value is "Standard".	
Availability Zone	Select Zone-redundant .	
Tier	Select Regional: ◦ Regional ◦ Global The default value is "Regional".	
IP address assignment	Select Static: ◦ Dynamic ◦ Static The default value is "Static".	

Parameter	Description	Length/Range
Routing preference	Select one of the following based on your preference: - Microsoft network - Internet The default value is "Microsoft network".	
Idle timeout (in minutes)	Enter the idle timeout in minutes. The default value is "4" minutes.	4-30 Minutes.
DNS label name	This is an optional field.	

- Click **review+create**.
- Verify the values.
- Click **Create**.

Generate Output Payload from createUIDefinition Sandbox

Related articles:

- [Installing RAMP on Azure Manually](#)
- [Checklist for Installing RAMP on Azure](#)

Use the following procedure to launch a Ribbon Application Management Platform (RAMP) instance using the Microsoft Azure Portal. Before you begin, make sure you have completed the steps that prepare your environment at [Checklist for Installing RAMP on Azure](#).

To instantiate a RAMP standalone instance on Microsoft Azure:

- Open the `CreateUIDefinition.json` file you downloaded from Ribbon in an editor and copy the entire contents of the file to your browser clipboard.
- Access the Microsoft Azure Portal and open the **Create UI Definition Sandbox** window.
- Replace any default contents that appear in the window with the contents of the `CreateUIDefinition.json` file.
- Click **Preview** to open the Sandbox GUI.
- Use the following table to specify the parameters you want to use for the RAMP instance you are creating.

Field	Description	Mandatory?
Basics – Project details		

Field	Description	Mandatory?
Subscription Resource Group	Select your Azure subscription and the resource group in which to create the virtual machine (VM) for the RAMP instance. Refer to Create a Resource Group for RAMP on Azure .	✓
Basics – Instance details		
Region	Select the region where you want to create the VM. Ribbon recommends selecting the region closest to the voice end user. If you plan to reuse an existing resource, select the region for the resource.	✓
Virtual Machine Name	Enter a name for the VM. This name is used as the hostname of the RAMP instance. Reuse the same name in case of upgrade/migration,	✓
Virtual Machine Settings – Azure VM size		
Virtual Machine Size	Select the VM size. The default is 1xStandard D16s v3, which includes 16 vcpus and 64 GB of memory.	✓
Image	Select the RAMP image file from the list. Ensure the image file is present in a resource group within your subscription to appear in the list. To obtain access to the image file on Azure, contact Ribbon Support.	✓
Network Settings – Configure virtual networks		
RAMP virtual network	Select an existing vnet, or create a new one, to act as a virtual private network that allows resources to communicate with each other securely. To create a new network when you are editing the RAMP template: a. Click the Create new link to open a Create virtual network pane where you can provide a name for the network. b. Click OK. The name of the new network appears as the RAMP virtual network and a new subnet is added.	✓

Field	Description	Mandatory?
Subnet	The subnet defines a particular range of IP addresses that will contain the RAMPprivate IP address. A subnet is also created when creating a new virtual network.	✓
Network Security Group	Select the name of the network security group you created for RAMP. This will contain the inbound and outbound access rules for RAMP. Refer to Create a Network Security Group for RAMP on Azure .	✓
RAMP Configuration Settings – RAMP Configuration User Interface		
Admin Public Key	This SSH key is generated on a Linux server to inject during instantiation to enable the admin user to access RAMP from that server without a password. To generate SSH key, refer to Generate SSH Keys for RAMP Users on Azure .	✓
Insight Public Key	This SSH key is generated on a Linux server to inject during instantiation to enable the insight user to access RAMP from that server without a password. To generate SSH key, refer to Generate SSH Keys for RAMP Users on Azure .	✓
RAMP Configuration Settings – RAMP System Identifiers		
DNS Host Name	The DNS server for the RAMP instance to use.	
NTP Server	The NTP server for the RAMP instance to use.	
Time Zone	The time zone for the RAMP instance.	
External Disk	Select the external disk you created to associate with the RAMP instance. Refer to Create an External Disk for RAMP on Azure . In case of upgrade or migration, re-use the same external disk used earlier.	✓

- Click the **Review + create** option.
- Select the **View output payload** option to open a **Template Parameters** pane showing the template settings in a JSON format.
- Copy the contents of the **Template Parameters** pane to your browser's clipboard.

You are now set to [Instantiate a Standalone RAMP Instance on Azure](#).

Installing RAMP CNF

In this section:

- [Helm Chart](#)
- [GitOps](#)

Related articles:

- [RAMP CNF - Standalone Deployment Using Helm Charts](#)
- [RAMP CNF - Standalone Deployment Using GitOps](#)

You can install the Ribbon Application Management Platform (RAMP) Cloud Native Functionality (CNF) using Helm charts and GitOps.

Helm Chart

Use the Helm chart to define, install, and upgrade RAMP CNF. Helm is the package manager for Kubernetes and uses a packaging format called charts. The Helm chart is a combination of multiple Kubernetes resource manifests that are combined into a single package that can be deployed in the Kubernetes cluster. For more information, refer to [RAMP CNF - Standalone Deployment Using Helm Charts](#).

GitOps

GitOps is a set of best practices and a methodology to manage infrastructure and applications in a declarative way. The core idea of GitOps is to use Git as a central repository to store the desired state of your infrastructure and applications and use automation (FluxCD) to keep the actual state of your system in sync with the desired state. For more information, refer to [RAMP CNF - Standalone Deployment Using GitOps](#).

RAMP CNF - Standalone Deployment Using GitOps

You can deploy Ribbon Application Management Platform (RAMP) Cloud Native Function (CNF) using the procedures outlined in this topic. The following workflow provides an overview of the process, including links to the specific information and steps required to complete the deployment. After completing the steps on the linked page, return to the workflow for the following procedure.

Step	Action
1	Review RAMP CNF - System Requirements to ensure your system has the necessary resources.
2	Review the RAMP CNF - Deployment Checklist Using GitOps to ensure you have the required information.
3	Complete the RAMP CNF - Install Using GitOps to install RAMP CNF using GitOps.

Step	Action
4	Review Check RAMP Status for post installation steps.

RAMP CNF - Deployment Checklist Using GitOps

In this section:

- [Create and Access Git Repository and Helm Artifactory](#)
- [Git RAMP CNF Helm Release File](#)
- [Git RAMP CNF Kustomization File](#)

Related article:

- [RAMP CNF - System Requirements](#)

You can deploy Ribbon Application Management Platform (RAMP) Cloud Native Function (CNF) using GitOps.

Prerequisites

- RAMP CNF Helm template is available in the Helm artifactory or Git repository.
- Application deployment tool (a CD tool, such as FluxCD) should be installed on the K8S cluster.
- Git repository for the helm manifest is available.
- Git permission to commit RAMP CNF related changes in the Helm manifest.

Create and Access Git Repository and Helm Artifactory

Create the Git repository, Helm artifactory, and container image artifactory in your lab or production environment and provide access.

Git RAMP CNF Helm Release File

Create the RAMP CNF deployment `.yaml` file based on the requirements.

Example:

```
# Values for RBBN-CORE-CNF chart
# This is a YAML-formatted file.
# Declare variables to be passed into your templates.

apiVersion: helm.toolkit.fluxcd.io/v2beta1
kind: HelmRelease
metadata:
  name: sanjay-blr-ramp
  namespace: ramp-svt
spec:
  releaseName: sanjay-blr-ramp
  targetNamespace: ramp-svt
  chart:
    spec:
      chart: rbbn-ramp-cnf
      version: 23.06.00-81
      sourceRef:
        kind: HelmRepository
```

```

    name: ramp-helm-prod-plano
    namespace: ramp-svt
install:
  disableWait: true
upgrade:
  disableWait: true
interval: 5m
timeout: 10m
values:
  global:

    # Namespace this helm chart will be deployed
    # This is optional. You could set to "" to use default namespace
    namespace: "ramp-svt"

    # Override obs storageClassName
    # This is optional. You could set to "" to use default storageClassName
    storageClassName: "managed-nfs-storage"

    ns_uuid: "8aebafe4-50c2-4f52-a43f-b7d1a40df51c"
    cnf_uuid: "e56aa2ea-2c1e-4964-970e-b86eaff727d9"
    cnfc_uuid: "b3e021dc-947d-4c19-824b-3412c267509f"

    certManager:
      enabled: true
      issuer:
        name: "cross-cluster-ca-selfsigned-clusterissuer"
        ## @param global.certManager.issuer.kind The Issuer kind to sign the
certificate request. Can be "Issuer" or "ClusterIssuer"
        kind: "ClusterIssuer"

    auth:
      kafkaClient:
        secureTransport: true
        certFilename: cert.pem
        certKeyFilename: key.pem
        caFilename: "ca.pem"

        ## @param auth.client.certDuration Requested duration the signed
certificate will be valid for
        certDuration: ""

        ## @param auth.client.certExtraDnsSans DNS Subject Alternative Name to add
to the certificates
        certExtraDnsSans: ""

        ## @param auth.client.certExtraIpSans IP Subject Alternative Name to add to
the certificates
        certExtraIpSans: ""

        ## @param auth.client.existingSecret Name of the existing secret containing
the TLS certificates for client-to-server communications
        existingSecret: ""

```

```

# Base RBBN_OBS container image.
# RCO: artifactory-tx.rbbn.com
# BLR: artifact2.eng.sonusnet.com
imageRegistry: artifact2.eng.sonusnet.com

# If you need kubernetes secret to pull from private repo. You will need
username and access token
# For example:
# To get the access token:
# curl -u <windowsUsername>:'<windowsPasswd>' -X POST https://
artifact2.eng.sonusnet.com/artifactory/api/security/token -d
"username=<windowsUsername>" -d "expires_in=86400" -d "refreshable=true" -d
"scope=member-of-groups:readers" -d "audience=jfirt*"
# Replace windowUsername and windowPassword with appropriate username and
password.
# set imageCredentials: {} if you don't secret to pull from private repo
imageCredentials:
  create: false
  #Private repo for ribbon images
  registry: artifact2.eng.sonusnet.com
  username: ssequeira
  password:
eyJ2ZXIiOiIyIiwidHlwIjoilSldUIiwiYWxnIjoilUMyNTYiLCJraWQiOiJ0b2Z0emxGZGtnSjdaWFZnRnRTT
m94RzBLMTE3ZEZldEVaVXd5YVg3a2xvIn0.eyJzdWIiOiJqZnJ0QDaxY2RxYnJwejljYzc1MXFnemI5bTIxaH
BlXC9lc2Vyc1wvc3NlcXVlaXJhIiwic2NwIjoibWVtYmVyLW9mLWdyb3Vwc3pyZWZkZXJzIiwiaXVkaWwIjoiamZ
ydEAqIiwiaXNzIjoiamZydEAwMWNkcWJycHo5Y2M3NTFxZ3piOW0yMWhwZVwvdXNlcnc3NzZXF1ZWlyYSIs
ImV4cCI6MTcxMTM2NjYzMiwiawWF0IjoxNjc5ODMwNjMyLCJqdGkiOiI3ODYwZjczMC1mODRkLTQyNjgtYmQ4N
C03MTc5MmUwZDFLZWEifQ.G_MdtWQsQqHEXz0X9L5wGvkk8HYnEfs87f0b1-5tcICeJ73B_aHIUYwFQRsa40y
kmtUDTmkDKTzT0kaQ8NCVstbLuFviRRgSxsafjPG4wdqnHZyF6Pq-NJZIsuKHGhtG59tHg1erq8nlyEAE-
_GHDVhivQtbsMfhAuFUJLG2xI8obeUWS8MWjQv2u301HPHcJv7QlIF8aX01p7EuqwmMidGnSM_wikwMT4cl4n
Abq0xh00y7glPVKE5TquKFH909vhzyWpvpSds0BCrMLTjR6Cy1wmvz5u5YiSS2rEG0q96j2KveSEYstJyVe1U
g0L_gnc4pv6Iie7Poc--pta4_Qg

# Override obs image for aggregator and agent
# This is required if you enable rbbn_obs (See below rbbn_obs.enabled = true)
obs:
  image:
    repository: ribbon-telemetry-docker-prod-plano/release/
rbbn-telemetry_collector
    tag: v1.3.5
    pullPolicy: Always

# Log rotation mechanism for the Observability server
obsLogRetentionPolicy:
# represent the percentage of the disk usage on when log rotation will be
trigger.
# I.e. A 20Gb storage limit request for a PVC with a rotateTriggerPercent
set at 50 (50%)
# means that log rotation will be trigger when disk will reach 10Gb
rotateTriggerPercent: 50
# Choice are "minute" "hourly" "daily" "weekly"
# recurringInterval represent the period of time on when we want to check if
disk usage has surpass the threshold.

```



```

    recurringInterval: "hourly"

    role:
      # Specifies whether a Role and RoleBinding should be created for the
observability components
      create: true

    serviceAccount:
      # Specifies whether a service account should be created for the
observability components
      create: false
      # Annotations to add to the service account
      annotations: {}
      # The name of the service account to use.
      # If not set and create is true, a name is generated using the fullname
template
      name: default

    # Storage request limit for PVC
logPersistentVolumeStorage:
      use: false
      request: 20Gi
      annotations:
        volume.beta.kubernetes.io/storage-provisioner: storage.io/nfs

    logs:
      # Name of secret that contains Elasticsearch credentials
      elasticsearchSecretName: ""
      # Name of secret that contains Elasticsearch credentials, evaluated as a
template, for example "{{.Release.Name }}-elasticsearch-user-cred"
      elasticsearchSecretNameTemplate: ""
      # Name of secret that contains Kafka credentials
      kafkaSecretName: ""
      # Name of secret that contains Kafka credentials, evaluated as a template,
for example "{{.Release.Name }}-kafka-user-cred"
      kafkaSecretNameTemplate: ""

      # Backend server configuration can be read here as an alternative to the
obs.logs section
      backendServers:

    #Timezone for ramp pod
    # This is optional. Comment it out if not needed. It will default to UTC if not
provided.
    timeZone: "Asia/Kolkata"

    # Platform on which the Ribbon RAMP CNE solution is deployed.
    # Allowed values - ocp, robin
    kubernetesPlatform: ocp

    # robin platform wants to be able to specify static_ip_policy in annotations
    # accepted values are ippool,range
    static_ip_policy: "ippool"

```

```

# Template strings to evaluate to existing secret to use to pull images, for
example: name: "{{.Release.Name }}-imagecred"
imagePullSecretTemplates:
  - name: "{{.Release.Name }}-imagecred"

# Values for rbbn-ramp chart
rbbn-ramp:
  #Ramp image
  # This is required
  rampImage:
    repository: ems-docker-prod-plano/production/rampcnf/rbbn-ramp-cnf
    pullPolicy: IfNotPresent
    # This is the ramp version
    tag: "23.06.00-81"
    #tag: "22.05.00-131"

# Define addition external interfaces for ramp pod
# This is required. Ramp requires eth1 for management access and eth2 for LI.
networkInterface:
  # Either 'ipv4' or 'ipv6'
  ipversion: "ipv4"
  #Number of external interface for ramp
  numberOfExternalInterface: 1
  # This is the interface for management access - devices, GR, etc.
  eth1:
    interface: ext-static-net-3
    ip: "10.52.80.129"
    prefix: "24"
    gateway: "10.52.80.1"
    routes:
      - destIp: 10.70.0.0
        prefix: "16"
      - destIp: 10.54.0.0
        prefix: "16"
      - destIp: 10.52.0.0
        prefix: "16"
      - destIp: 10.32.0.0
        prefix: "16"
      - destIp: 10.34.0.0
        prefix: "16"
      - destIp: 10.33.0.0
        prefix: "16"
      - destIp: 172.21.0.0
        prefix: "16"
      - destIp: 172.19.0.0
        prefix: "16"
      - destIp: 172.29.0.0
        prefix: "16"
  # This is the interface for LI
  eth2:
    interface: ext-static-net-4
    ip: ""

```

```

    prefix: ""
    gateway: ""
    routes:
      - destIp: ""
        prefix: ""

    # Ramp kubernetes service
    # "port" exposes the Kubernetes service on the specified port within the
    cluster. Other pods within the cluster can communicate with this server on the
    specified port
    # "type" could be "ClusterIP", "NodePort" and "LoadBalancer". Refer to
    kubernetes service for more detail.
    # Set enabled: false if not needed.
    rampService:
      enabled: false
      port: 443
      type: ClusterIP

    auth:
      # etcd client TLS certificate
      etcdclient:
        certManager:
          # enabled: switch to enable cert-manager to generate and manage the etcd
          client certificate
          # NOTE: Set this to true only if global.certManager.enabled is set to
          true and network.interfaceName
          # is set to eth1 and the network attachment used for eth1 is configured
          to assign static IPs.
          enabled: true
          ## @param auth.client.certExtraDnsSans DNS Subject Alternative Name to
          add to the certificates
          ##
          certExtraDnsSans: ""
          ## @param auth.client.certExtraIpSans IP Subject Alternative Name to add
          to the certificates
          ##
          certExtraIpSans: ""
          # certDuration: duration in hours, minutes, or seconds that the
          certificate should be valid for
          # NOTE: If certDuration is not specified (""), then the certificate will
          be valid
          # for 90 days by default and will be renewed 30 days before expiry. The
          minimum value for
          # certDuration is 1 hour.
          # Example:
          # If the duration needs to be 180 days, then this can be specified as
          below:
          #   certDuration: 4320h
          certDuration: ""

    alarm:
      exporters:
        - enabled: false

```

```

    type: kafka
    config:
      bootstrap_servers:
        - ip: 127.0.0.1
          port: 9092
      topic: ""
      format: json
      standard: ETSI_S0L003
      properties: # producer configuration can be provided here with proper
indentation
        # security.protocol: SSL
        # ssl.kafka.private.key.location: /opt/fm/kafka/certs/key.pem
        # ssl.kafka.public.cert.location: /opt/fm/kafka/certs/cert.pem
        # ssl.kafka.ca.cert.location: /opt/fm/kafka/certs/ca.pem

    # The memory/cpu limits will be equals to requests to esure pod gets assigned a
QoS class of Guaranteed
    # Required
    rampResources:
      requests:
        cpu: 16
        memory: 64Gi
    # hugepages:
    limits:
    # hugepages: 2Gi

    # Persistent for ramp container
    rampPersistent:
      #Storage class class for ramp. User could configure diffirent
storageClassName for obs(global section)
      #storageClass is optional field.
      #storageClassName is optional. Comment it out if you want to use default
storageClassName.
      storageClassName: "csi-rbd-sc"

      # storageAccessMode for ramp
      #ReadWriteOnce - the volume can be mounted as read-write by a single node
      #ReadOnlyMany - the volume can be mounted read-only by many nodes
      #ReadWriteMany - the volume can be mounted as read-write by many nodes
      # storageAccessMode is required field
      storageAccessMode: "ReadWriteOnce"

      # Storage size. Required field.
      storage: "130Gi"

    # Enable or disable startupProbe, livenessProbe, and readinessProbe
    probe: True

    #Assigning Pods to Nodes with specific label
    #For example:
    nodeSelector: {}
    #nodeSelector:
    # kubernetes.io/hostname: worker-9.blr-ocp1.lab.rbbn.com

```

```

# Set this for kubernetes tolerations
# Optional
tolerations: []

# Set this for kubernetes affinity
# Optional
affinity: {}

# Set the namespaces for antiaffinity rule
anti_affinity_namespaces: ["ramp-svt", "sbc-svt-regr", "psx-svt", "ems-dev",
"ems-svt-perf", "ems-svt", "ats-dev", "ems-svt-2", "platform-dev", "platform-svt", "psx-
dev", "raf-dev", "rampev-svt", "sbx-dev", "sbc-svt", "psx-cnf-svt", "cnf-demolab", "sbc-
dev-tekton", "ramp-svt", "ems-svt-perf", "cats-svt"]

#Use this to inject public keys for users. Set it to
# Optional
#Users: [] if not needed.
users:
- name: "admin"
  # To generate password for "admin" user, run "openssl passwd -6 admin"
  password: "$6$lQMeZQPJJoAXfchXn$2jYBgDqj9ubRTRMgPwoDQg87358IBY7pV9FmBf/
VNN57htb0WP9DezDgXp30mo7LthuHbDjFekrAWxB8UQ/tt1"
  ssh_authorized_keys:
    - ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIE1q9aASBnezCE+irhepjRZSuY4wOhkNBUyQ0uqnCgeT admin@rbbn.com
- name: "insight"
  # To generate password for "insight" user, run "openssl passwd -6 insight"
  password: "$6$WDZgaeEQY007xZLg$SVZ/OQL/.VUF/dFu/
1M.rxfNq0JdxSXNHciPqKwduuyoS0y6iLnN2kZ/qbLhMVVDwarQYmbCB22C9pGZ.BT8f1"
  ssh_authorized_keys:
    - ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIE1q9aASBnezCE+irhepjRZSuY4wOhkNBUyQ0uqnCgeT insight@rbbn.com

# You only need to modify this if you want to use rbbn-sdrp
# Set enabled: true if you want to enable sdrp for ramp. Default to false
rbbn_sdrp:
  enabled: false
  fqdn_instance: ""

# You only need to modify this if you want to use rbbn-obs
# Set enabled: true if you want to enable observability agent for ramp. Default
to true
rbbn_obs:
  enabled: true

# Service for obs sidecar within pod.
obsService:
  type: ClusterIP
  port: 9101
  ipFamilyPolicy: SingleStack # Allowed values PreferDualStack or
SingleStack.According the below value should be altered
  ipFamilies:

```

```

- IPv4

resources:
  rbbn_telemetry_agent:
    limits:
      cpu: 4
      memory: 8Gi
    #requests:
    #  cpu: 100m
    #  memory: 128Mi

# Add the pod annotations to enable prometheus discovery and scraping.
# port we are exposing for prometheus scraping.
# This port should match the service port and the server metric output
endpoint.
podAnnotations:
  prometheus.io/path: "/metrics"
  prometheus.io/scrape: true
  prometheus.io/port: "9101"
  prometheus.io/scheme: "http"

serviceLabels:
  component: prometheus-rbbn-otel-agent
  tenant: ramp
  servicetype: observability

configMap:
  metrics:
    enable: True
    appStats:
      scrapeInterval: 5s
      endpoints:
        - addr: "localhost:10050"
          containerName: rbbn-rampcnf-container
      output:
        - server: "prometheus"
          endpoint: "0.0.0.0:9101"
  logs:
    enable: True
    defaultTopic: default # log messages to this Kafka topic by default when
a topic for the container parsers or system is not specified
    system: True
    systemTopic: system # system logs will be sent to this Kafka topic,
defaultTopic is used if this property is not defined
    telemetry:
      enable: True # Process the otel agent logs
      topic: rbbn-otel-agent # Open telemetry logs will be sent to this Kafka
topic
    podlogs: True
    logPrefix:
      nodeId: True
      containerId: True

```

```

kafkaSecretName: ""
backendServers: # Example of backend servers
  stdout:
    enable: False
  elasticsearch: []
    # - endpoint: elasticsearch.apps.rco-ocp1.lab.rbbn.com:443
    #   auth: True
    #   username: ELASTICSEARCH_USER
    #   password: ELASTICSEARCH_PASSWD
    #   index: platform-filebeat
  kafka: []
    # - endpoint: elasticsearch.apps.rco-ocp1.lab.rbbn.com:12345
    #   sslCert: KAFKA_CERT
    #   sslKey: KAFKA_KEY
    #   sslCa: KAFKA_CA
# elasticsearch Credentials
elasticsearchCreds:
  create: False
  #user:
    #key: ELASTICSEARCH_USER
    #value:
  #password:
    #key: ELASTICSEARCH_PASSWD
    #value:
# KAFKA Credentials
# all values should be base64 encoded.
kafkaCreds:
  create: False
  path: /etc/kafka/ssl
  sslCert:
    key: KAFKA_CERT
    value:
  sslKey:
    key: KAFKA_KEY
    value:
  sslCa:
    key: KAFKA_CA
    value:

## sdrp subchart values
sdrp-operator:
  common-util:
    logPersistentVolumeStorage:
      create: false
    imageCredentials:
      # Specifies whether an image credentials secret should be created as a post-
delete hook
      createPostDelete: true

## @section sdrp-operator container parameters
operator:

## @param sdrp-operator image parameters

```

```

image:
  ## @param operator.image.repository sdrp-operator image name
  repository: ccs-docker-prod-virtual/sdrp-operator

  ## @section sdr container parameters
  ##
  ## @param sdr.clusterScopeRegistry.enabled Create a backend configuration for
the cluster scope if equal true
  ## @param sdr.globalScopeRegistry Specify the initial backend configuration for
the global scope to use in the sdr container
  ## @param nameservers - [array] List of DNS nameserver. Syntax: ip:port. If
port if not specified, port 53 is used
  ## @param domain - Name of the domain to publish to in the service registry for
the cluster scope
  ## @param tsigKeyName - Name of the TSIG key attached to DNS messages
  ## @param tsigSecret - TSIG (base64) value attached to DNS messages
  ## @param tsigSecretAlg - TSIG algorithm. Supported value: hmac-md5, hmac-sha1,
hmac-sha256, hmac-sha512
  ##
  sdr:
    ## @param sdrp-operator image parameters
    image:
      ## @param operator.image.repository sdrp-operator image name
      repository: service_discovery-docker-prod-ottawa/sdr

clusterScopeRegistry:
  enabled: true
  nameservers: []
  domain: ""
  tsigKeyName: ""
  tsigSecret: ""
  tsigSecretAlg: ""
globalScopeRegistry:
  enabled: true
  nameservers: []
  domain: ""
  tsigKeyName: ""
  tsigSecret: ""
  tsigSecretAlg: ""

```

Git RAMP CNF Kustomization File

Create the `kustomization.yaml` file to include the RAMP CNF deployment file name.

```

apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization
nameSuffix: -ssequeira
resources:
  - values_ramp.yaml ---> This is the name of the HelmRelease file

```


RAMP CNF - Install Using GitOps

In this section:

- [RAMP CNF Install Using GitOps](#)
- [RAMP CNF Git Deployment Monitoring](#)
- [RAMP CNF GIT Deployment Status](#)
- [Post-Installation Check](#)

Related articles:

- [RAMP CNF - System Requirements](#)
- [RAMP CNF - Deployment Checklist Using GitOps](#)

You can install and monitor the Ribbon Application Management Platform (RAMP) Cloud native Functionality (CNF) installation using the following procedures.

Prerequisite

Fulfill the requirements in the [RAMP CNF - Deployment Checklist Using GitOps](#).

RAMP CNF Install Using GitOps

Complete the following procedure to deploy RAMP CNF using GitOps.

Start

1. Commit the changes using the command:

```
git commit
```

2. Push the committed changes using the command:

```
git push
```

Example:

```
[ssequeira@cli-blr-2 jenkinsbuild-dev]$ git add -A; git commit -a -m "installing ramp"; git push origin master
[master 88562d8] installing ramp
 1 file changed, 1 insertion(+), 1 deletion(-)
Counting objects: 11, done.
Delta compression using up to 24 threads.
Compressing objects: 100% (5/5), done.
Writing objects: 100% (6/6), 530 bytes | 0 bytes/s, done.
Total 6 (delta 3), reused 0 (delta 0)
To ssh://git@bitbucket.rbbn.com:7999/ems/rbbn-cnf-gitops-ramp-svt.git
 01f6ef4..88562d8 master -> master
[ssequeira@cli-blr-2 jenkinsbuild-dev]$
```

RAMP CNF Git Deployment Monitoring

Use the following procedure to monitor the deployment in the Kubernetes cluster.

Start

1. Get the repository where the file is located:

```
oc get gitrepository
```

Example:

```
[ssequeira@cli-server ssequeira]$ oc get gitrepository
NAME                                URL
AGE   READY   STATUS
rbbn-cnf-gitops-ramp-svt  https://bitbucket.rbbn.com/scm/ems/rbbn-cnf-gitops-
ramp-svt.git  44d   True    stored artifact for revision 'master/
01f6ef4487b66e0b3d6647819e7b127f8537ea07'
```

2. Get the kustomization file:

```
oc get kustomization
```

Example:

```
[ssequeira@cli-blr-2 ~]]$ oc get kustomization
NAME                                AGE   READY   STATUS
rbbn-cnf-gitops-ramp-svt-ssequeira  43d   True    Applied revision: master/
01f6ef4487b66e0b3d6647819e7b127f8537ea07
```

3. Get the Helm chart for this installation:

```
oc get helmchart
```

Example:

```
[ssequeira@cli-blr-2 ~]$ oc get helmchart
NAME                                CHART                                VERSION   SOURCE
KIND      SOURCE NAME                        AGE   READY   STATUS
cnf-demo-lab-lpl-blr1-ramp-ssequeira  v23.06.00-94/                      *
GitRepository  rbbn-sbccore-cnf-manifests  6m19s   True    packaged 'rbbn-core-
cnf' chart with version '12.0.0-14505'
```

4. Get the release specific Helm chart:

```
oc get helmrelease
```

Example:

```
[ssequira@cli-blr-2 ~]$ oc get helmrelease
NAME                                AGE    READY    STATUS
lpl-blr1-ramp-ssequira             6m37s  True     Release reconciliation
succeeded
```

- List the Helm charts:

```
helm ls
```

Example:

```
[ssequira@cli-blr-2 ~]$ helm ls
NAME              NAMESPACE    REVISION    UPDATED
STATUS           CHART          APP VERSION
sanjay-blr-ramp   ramp-svt 1    2023-05-30 10:16:20.895043071 +000
0 UTC deployed   rbbn-ramp-cnf-23.06.00-94  1.0
```

- Check the installation status:

```
helm history sanjay-blr-ram
```

Example:

```
[ssequira@cli-blr-2 ~]$ helm history sanjay-blr-ramp
REVISION    UPDATED              STATUS    CHART
APP VERSION  DESCRIPTION
1           Wed Jun 21 22:11:29 2023  deployed  rbbn-ramp-cnf-23.0
6.00-94     1.0                  Install complete
```

RAMP CNF GIT Deployment Status

Use the following procedure to check the deployment status.

Start

- Check the deployment status:

```
oc get pods
```

Example:

```
[ssequeira@cli-blr-2 ~]$ oc get pods
sanjay-blr-ramp-rampcnf-0          2/2      Running    0      18h
```

Post-Installation Check

After a successful deployment, check the status of RAMP using [RAMP CNF - Post Installation Steps](#).

RAMP CNF - Standalone Deployment Using Helm Charts

In this section:

- [RAMP CNF - Deployment Checklist Using Helm Charts](#)
- [RAMP CNF - Install Using Helm Charts](#)

Related article:

[RAMP CNF - System Requirements](#)

You can deploy Ribbon Application Management Platform (RAMP) Cloud Native Function (CNF) using the procedures outlined in this topic. The following workflow provides an overview of the process, including links to the specific information and steps required to complete the deployment. After completing the steps on the linked page, return to the workflow for the next procedure.

Step	Action
1	Review RAMP CNF - System Requirements to ensure your system has the necessary resources.
2	Review the RAMP CNF - Deployment Checklist Using Helm Charts to ensure you have the required information.
3	Complete the RAMP CNF - Install Using Helm Charts to install RAMP CNF using Helm charts.
4	Review RAMP CNF - Post Installation Steps .

RAMP CNF - Deployment Checklist Using Helm Charts

Related articles:

- [RAMP CNF - System Requirements](#)
- [RAMP CNF - Standalone Deployment Using Helm Charts](#)

To deploy the Ribbon Application Management Platform (RAMP) Cloud Native Functionality (CNF), ensure the following:

- All the images are available in the artifactory.
- Download the Helm chart, it is available as part of the tarball in the artifactory.
- Update the `values.yaml` file with the mandatory details:
 - Details about the IP addresses and gateways used.
 - Provide the network or prefix of all the devices that you may want to register with RAMP if they are not within the same broadcast domain.
- The settings for maximum user instances and container pod limits are to be updated on the worker nodes before deploying the RAMP CNF:
 - `fs.inotify.max_user_instances = 8192`
 - `sysctl kernel.pid_max >= 4096`
- Create roles, role bindings, and service accounts as part of the kubernetes cluster,

To instantiate your deployment using Helm charts, provide parametric values to configure the Helm chart. Before you instantiate the deployment, review the parameters in the following table to collect mandatory values and determine the optional parameters you want to configure.

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
.Values.global						
	namespace	Yes	String	NA	NA	The namespace/project where the RAMP CNF solution will be deployed.
	storageClass Name	Yes	For details, see " <code>oc get storageclasses</code> ".	NA	NA	The storage class for PVCs used by the Observability Container.
	ns_uuid	No	String	NA	NA	The namespace ID, where the RAMP CNF pod is spawned.
	cnf_uuid	No	String	NA	NA	The RAMP pod ID.
	cnfc_uuid	No	String	NA	NA	The container ID.

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	certManager: enabled: false issuer: name: "" kind: ""	No	String	ClusterIssuer	ClusterIssuer or Issuer	This is required for issuing the SSL certificates. If certificate manager is unavailable certificates can also be provided using secret. Needed for providing SSL certificates. If the certificate manager is unavailable, then certificates are provided using secret.

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	activedirectory: enabled: false hostAliases: - ip: "" hostnames: - "" - "" - ip: "" hostnames: - "" - "" dnsConfig: nameservers: - "" # searches: # - # options: # - name: ndots # value: "2"	No		<pre>## @param activedirectory to enable activedirectory ## set enabled to true to use activedirectory activedirectory: enabled: false ## @param hostAliases add more list parameters as required hostAliases: - ip: "" hostnames: - "" - "" - ip: "" hostnames: - "" - ""</pre>		To configure active directory, refer to Custom Host and DNS Configuration for Kubernetes Pods .

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
				<pre>## @param dnsConfig for activeDirectory dnsConfig: ## @param nameservers add more list parameters as required nameservers: - "" # searches: # - # options: # - name: ndots # value: "2"</pre>		
	auth: kafkaClient: secureTransport: false certFilename: cert.pem certKeyFilename: key.pem caFilename: "ca.pem" certDuration: "" certExtraDnsSans: "" certExtraIpSans: "" existingSecret: ""	No		secureTransport(false) certFilename(cert.pem) certKeyFilename(key.pem) caFilename(ca.pem)	secureTransport(false,true)	If secure transport is enabled then the certificates are provided by the certificate manager or using secret. If certificate manager is used to provide the certificates then, names of cert file, private key file, CA certificate file are needed in the <code>values.yaml</code>. Here <code>certDuration</code> is in hours, for example, "720h". If certificate manager is not used then <code>existingSecret</code> attribute has the name of the secret, this mounts all the required certificates in the container.

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	imageCredentials:	Yes	Name, registry, username, and password.	NA	NA	Used to access the artifactory for docker images. For the password, generate the token as per the details provided in the Artifactory Removal of Anonymous Access - Engineering Tools and Admin - Ribbon Employee Wiki (rbbn.com).image credentials for RAMP Helm charts.
	timeZone:	Yes	String	UTC		If the values are not provided, then the system defaults to UTC. Set this to one of the values in the "TZ identifier" column in the list of timezones at https://en.wikipedia.org/wiki/List_of_tz_database_time_zones .
	kubernetesPlatform:	Yes	String	ocp	ocp, robin	This is the platform on which RAMP is deployed.
	static_ip_policy	Yes	String	ippool	ippool, range	The <code>static_ip_policy</code> in robin annotations.
	imagePullSecretTemplates:	Yes	String	name("{{.Release.Name }}-imagecred")		The template strings to evaluate the existing secret used to pull images. For example, name: <code>"{{.Release.Name }}-imagecred"</code> .
.Values.global.obs						

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	image: tag: pullPolicy:	Yes	tag(v1.0.0) pullPolicy(Always)			Image: The OBS image location in the artifactory. For example, artifact2.eng.sonusnet.com/ ribbon_telemetry-docker- prod-plano/release/ rbbn_telemetry_collector.
	obsLogRetentionPolicy: rotateTriggerPercent: recurringInterval:	Yes		rotateTriggerPercent(50) recurringInterval(hourly)	recurringInterval ("minute", "hourly", "daily", "weekly")	This is the log rotation mechanism for the Observability server. rotateTriggerPercent: represents the percentage of the disk usage that triggers log rotation. For example, a 20Gb storage limit request for a PVC with a <code>rotateTriggerPercent</code> set at 50 (50%) means that log rotation triggers when the disk reaches 10Gb. recurringInterval: represents time frame from when you want to check if disk usage has surpass the threshold.
	role: create: true	No	boolean	create(true)	create(true,false)	Specifies if a Role and <code>RoleBinding</code> is to be created for observability components.
	serviceAccount: create: false annotations: { name: default	No	NA	NA	NA	Specifies if a service account is to be created for the observability components. If a name is not set and create is true, a name is generated using the fullname template.

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	ogPersistentVolumeStorage: request: 20Gi annotations	NA	NA	request(20Gi)	NA	The storage request limit for OBS PVC.
Values.global.obs.logs						
	elasticsearchSecretName:	No	String	NA	NA	Name of secret that contains Elasticsearch credentials
	elasticsearchSecretNameTemplate:	No	String	NA	NA	Name of secret that contains Elasticsearch credentials, evaluated as a template. Example: "{{.Release.Name }}-elasticsearch-user-cred"
	kafkaSecretName:	No	String	NA	NA	Name of secret that contains Kafka credentials.
	kafkaSecretNameTemplate:	No	String	NA	NA	Name of secret that contains Kafka credentials, evaluated as a template, for example "{{.Release.Name }}-kafka-user-cred".
	backendServers:	No	NA	NA	NA	This is an alternative to the .Values.rbbn-ramp.rbbn_obs.logs, the backend server configurations are available here.
rbbn-ramp						

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	ramplImage: repository: tag: pullPolicy:	Yes	Repository Name and the Image tag.	pullPolicy(IfNot Present)	NA	This is the repository, image pullPolicy, and image tag for the RAMP image.
	networkInterface: ipversion: numberOfExternalInterface: 1 eth1: interface: ip: prefix: "24" gateway: "10.52.84.1" routes: - destIp: prefix:	Yes	NA	ipversion(ipv4)	ipversion ('ipv4' or 'ipv6')	Define additional external interfaces for RAMP pod: • eth1: is for management access. • eth2: is for LI. • interface: the name of the network attachment definition • The routes field should have the list of external networks that the devices to be registered will belong to.

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	auth: etcdclient: certManager: enabled: true certExtraDnsSans: certExtraIpSans: certDuration:	Yes	NA	NA	NA	- enabled: the switch to enable cert-manager to generate and manage the etcd client certificates. NOTE: Set this to true only if global.certManager.enabled is set to true and network.interfaceName is set to eth1 and the network attachment used for eth1 is configured to assign static IPs certExtraDnsSans: the DNS Subject Alternative Name to add to the certificates. certExtraIpSans: the IP Subject Alternative Name to add to the certificates. certDuration: the duration in hours, minutes, or seconds that the certificate should be valid for. NOTE: If certDuration is not specified (""), then the certificate is valid for 90 days by default and renewed 30 days before expiry. The minimum value for certDuration is 1 hour.

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	alarm: exporters: - enabled: false type: kafka config: bootstrap_servers: - ip: 127.0.0.1 port: 9092 topic: "" format: json standard: ETSI_SOL003 properties:	No	NA	format(json) standard(ETSI_SOL003)	NA	Enable this configuration when traps to RAMP are to be exported to kafka. • topic: the name of the topic • properties: consists of all the producer properties required. You can use producer configurations from: https://kafka.apache.org/documentation/#producerconfigs
	rampResources: requests: cpu: memory:	Yes	NA	cpu(16) memory(64Gi)	NA	Cpu and memory for request and limit. The memory/cpu limits will be equals to requests to ensure pod gets assigned a QoS class of Guaranteed.
	rampPersistent: storageClassName:: storageAccessMode: storage:	Yes	NA	storageAccessMode("ReadWriteOnce") storage("130Gi")	NA	Persistent for RAMP. RAMP <code>storageClassName</code> is configured here.

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	probe:	Yes	True	NA	NA	Enable or disable startupProbe, livenessProbe, and readinessProbe.
	nodeSelector:	No	NA	{}	NA	Assigning Pods to Nodes with a specific label. For example, <pre>nodeSelector: kubernetes.io/hostname: worker-9.blr-ocp1.lab.rbbn.com</pre>
	tolerations:	No	NA	[]	NA	Set this for kubernetes tolerations.
	affinity:	No		{}	NA	Set this for kubernetes affinity.
	anti_affinity_namespaces:	Yes	List	["ems-dev","ems-svt"]	NA	Set the namespaces for anti-affinity rule.
	users: - name: "admin" password: ssh_authorized_keys:	No	List	The default password and ssh key are provided for admin and insight users in <code>values.yaml</code> .	NA	Use this to provide public keys for users.
	rbbn_sdrp: enabled: false fqdn_instance: ""	No	NA	enabled(false)	NA	Set "enabled" as true if you want to enable sdrp for RAMP. Set the default value as "false".
rbbn-ramp.rbbn_obs						

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	enabled:	Yes	Yes	enabled(true)	enabled(true,false)	Enable this to bring obs container along with RAMP container.
	resources: rbbn_telemetry_agent: limits: cpu: 4 memory: 8Gi	Yes	NA	cpu(4) memory(8Gi)	NA	This is the configuration for OBS container resources.
	podAnnotations: prometheus.io/path: "/" metrics" prometheus.io/scrape: true prometheus.io/port: "9101" prometheus.io/scheme: "http"	No	NA		NA	Add pod annotations to enable prometheus discovery and scraping. The port you expose for prometheus scraping must match the service port and the server metric output endpoint.
rbbn-ramp.rbbn_obs.configMap.metrics						
	enable: True	Yes	NA	enable(True)	NA	If this is enables, the obs agent collects system metrics from RAMP container based on the configured interval.
rbbn-ramp.rbbn_obs.configMap.logs						
	defaultTopic: default	Yes	NA	defaultTopic(default)	NA	This is the default value, if the container parsers or system is not specified.

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	systemTopic:	No	NA	systemTopic(system)	NA	System logs are sent to this Kafka topic. The defaultTopic is used if this property is not defined.
rbbn-ramp.rbbn_obs.configMap.logs.logPrefix						
	nodeId: True	Yes	NA	True		Set the node ID to true.
	containerId: True	Yes	NA	True		Set the container ID to true.
rbbn-ramp.rbbn_obs.configMap.logs.backendServers						
	stdout: enable: False	No	NA	False	True or False	Update this configuration to export logs to stdout.
	elasticsearch:	No	NA	[]	No	Add this configuration to export logs to elastic search. For secured communication, add details under <code>.Values.rbbn_obs.elasticsearchCreds</code>
	kafka:	No	NA	[]	NA	Add this configuration to export logs to kafka. For secured communication, add details under <code>.Values.rbbn_obs.kafkaCreds</code>
sdrp-operator	NA	NA	NA	NA	NA	Node_name included as a prefix to the file and tagged to EFK.
sdrp-operator.sdr	NA	NA	NA	NA	NA	Container_name included as a prefix to the file and tagged to EFK

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	clusterScopeRegistry: enabled: true nameservers: domain: tsigKeyName: tsigSecret: tsigSecretAlg:	No	NA	NA	NA	• sdr.clusterScopeRegistry.enabled: creates a backend configuration for the cluster scope if the value is true. • nameservers: [array] List of DNS name servers. The syntax is: ip:port. If port is not specified then port 53 is used. • domain: name of the domain to publish to in the service registry for the cluster scope. • tsigKeyName: name of the TSIG key attached to DNS messages. • tsigSecret: TSIG (base64) value attached to DNS messages. • tsigSecretAlg: TSIG algorithm. ◦ Supported values: hmac-md5, hmac-sha1, hmac-sha256, hmac-sha512

Section	Name	Mandatory	Type/Value	Default Value	Accepted Values	Description
	globalScopeRegistry: enabled: true nameservers: domain: tsigKeyName: : tsigSecret: tsigSecretAlg:	No	NA	NA	NA	• sdr.globalScopeRegistry : specifies the initial backend configuration for the global scope to use in the sdr container. • nameservers: [array] List of DNS nameserver. ◦ The syntax is: ip:port ◦ If port is not specified, port 53 is used • domain: name of the domain to publish to in the service registry for the cluster scope. • tsigKeyName: name of the TSIG key attached to DNS messages. • tsigSecret: TSIG (base64) value attached to DNS messages • tsigSecretAlg: TSIG algorithm. ◦ Supported values: hmac-md5, hmac-sha1, hmac-sha256, hmac-sha512.

RAMP CNF - Install Using Helm Charts

Related articles:

- [RAMP CNF - Standalone Deployment Using Helm Charts](#)
- [RAMP CNF - Deployment Checklist Using Helm Charts](#)

Install RAMP CNF Using Helm Charts

Complete the following procedure to deploy the Ribbon Application Management Platform (RAMP) Cloud Native Function (CNF) using Helm charts.

1. Download the tarball from the artifactory. Refer to [Download Files from Ribbon Support Portal](#) for instructions for downloading files from Ribbon.
2. Navigate to the root directory of the Helm chart:

```
cd <root directory of the Helm chart>
```

3. Install RAMP CNF using Helm:

```
helm install <release_name> <root directory of the Helm chart>
```

Example:

```
[user@cli-server rbbn-ramp-cnf]$ helm install sanramprco2 -f values.yaml .
I0523 13:15:52.950511 7554 request.go:668] Waited for 1.165562433s due to
client-side throttling, not priority and fairness, request: GET:https://api.rco-
ocp1.lab.rbbn.com:6443/apis/autoscaling.openshift.io/v1?timeout=32s
NAME: sanramprco2
LAST DEPLOYED: Tue May 23 13:15:56 2023
NAMESPACE: ems-svt
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
```

4. List the pods in the Helm chart:

```
oc get pod -o wide
```

Example:

```
[user@cli-server ~]$ oc get pod -o wide
```

NAME	READY	STATUS	RESTARTS	AGE	IP
sanramprco2-rampcnf-0	2/2	Running	1 (4h11m ago)	4h36m	10.231.13.209
worker-3.rco-ocp1.lab.rbbn.com		<none>		<none>	

```
[user@cli-server ~]$
```

RAMP CNF - Post Installation Steps

After you install the Ribbon Application Management Platform (RAMP) for CNF, perform the following post-installation procedure to set the **Randomize Poll START Offset Secs** field to "70":

Prerequisite

Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Administration > Collector**.
3. Update **Randomize Poll START Offset Secs** to 70.
4. Click **Save**.

Generate Certificate Authority

Introduction

The ETCD supports automatic TLS authentication through client certificates for client-to-server and peer (server-to-server / cluster) communication. The ETCD certificates can be generated using a cert-manager, an extensible X.509 certificate controller for Kubernetes, or the certificates can be generated using existing Secret. Initially, a CA certificate and a signed key pair are required for one member. A new pair of keys for creating and signing for every member is required. The ETCD instances require two sets of TLS certificates: one certificate to serve client requests and a second for the peer endpoint used for communication between members. Use the below procedure to generate the CA certificate.

The CFSSL, CloudFlare's PKI/TLS utility, is a versatile tool for managing certificates. It offers a command-line interface and an HTTP API server for signing, verifying, and bundling TLS certificates.

Generate Certificate Authority

Prerequisites

- The **CFSSL** utility is the primary command-line tool for using the CFSSL packages. The CFSSL version should be 1.2.0 and above.
- The **cfssljson** utility processes the JSON output from **cfssl**, writes certificates, keys, Certificate Signing Requests (CSRs), and bundles to disk.
- To download cfssl on the x86_64linux host, run the following command:

```
mkdir ~/certs
curl -s -L -o ~/certs/cfssl https://pkg.cfssl.org/R1.2/cfssl_linux-amd64
curl -s -L -o ~/certs/cfssljson https://pkg.cfssl.org/R1.2/cfssljson_linux-amd64
chmod +x ~/certs/{cfssl,cfssljson}
export PATH=$PATH:~/certs
```

To verify the CFSSL version, run the below command:

```
$ cfssl version
Version: 1.2.0
```

```
Revision: dev
Runtime: go1.6
```

To create a directory, hold your certificates and private keys. This is required to generate more certificates.

```
cd ~/certs
echo '{"CN":"CA","key":{"algo":"rsa","size":2048},"names":
[{"C":"JP","L":"Kiba","O":"Rakuten Mobile Testing","OU":"IMS","ST":"Setagaya-ku"}]}' |
cfssl gencert -initca - | cfssljson -bare ca -
echo '{"signing":{"default":{"expiry":"43800h","usages":["signing","key
encipherment","server auth","client auth"]}}}' > ca-config.json
```

Example Output:

Example Output:

```
# cd ~/certs
# echo '{"CN":"CA","key":{"algo":"rsa","size":2048},"names":
[{"C":"JP","L":"Kiba","O":"Rakuten Mobile Testing","OU":"IMS","ST":"Setagaya-ku"}]}' |
cfssl gencert -initca - | cfssljson -bare ca -
2024/05/14 12:39:59 [INFO] generating a new CA key and certificate from CSR
2024/05/14 12:39:59 [INFO] generate received request
2024/05/14 12:39:59 [INFO] received CSR
2024/05/14 12:39:59 [INFO] generating key: rsa-2048
2024/05/14 12:40:00 [INFO] encoded CSR
2024/05/14 12:40:00 [INFO] signed certificate with serial number
405377637514415405541947339092037159882990300708

# echo '{"signing":{"default":{"expiry":"43800h","usages":["signing","key
encipherment","server auth","client auth"]}}}' > ca-config.json
# ls -ltr
total 12380
-rwxr-xr-x 1 root root 10376657 May 14 12:39 cfssl
-rwxr-xr-x 1 root root 2277873 May 14 12:39 cfssljson
-rw-r--r-- 1 root root 1383 May 14 12:40 ca.pem
-rw----- 1 root root 1679 May 14 12:40 ca-key.pem
-rw-r--r-- 1 root root 1013 May 14 12:40 ca.csr
-rw-r--r-- 1 root root 112 May 14 12:40 ca-config.json
#
```

Install and Configure Ribbon OEM Host OS for RAMP on Dell Server

Ribbon provides a Red Hat Enterprise Linux (RHEL) HOST OS software to use on specific third-party servers such as Dell ordered by Ribbon Customers for use with Ribbon Applications. The RHEL security-hardened OS is called Ribbon OEM Host OS (ROHOS).

Various Ribbon products are deployed on hardware platforms with a variety of processor, memory, and storage options. These servers are supplied directly to customers with the Ribbon OEM Host OS installed. This guide includes the procedures to install, update, configure, back up, and restore the Ribbon OEM Host OS.

Links to install and update topics:

Install Ribbon OEM Host OS	Install the Ribbon OEM HOST OS using the iDRAC management console (for Dell servers).
Update Ribbon OEM Host OS Software	Update the Ribbon OEM Host OS software and verify the update.
Configure Ribbon OEM Host OS Network	Configure the management interface, hostname, time zone and time server using the Ribbon network configuration tool.
Back Up Ribbon OEM Host OS	Perform a backup of the Ribbon OEM Host OS using an NFS server.
Restore Ribbon OEM Host OS	Restore the Ribbon OEM Host OS using the ISO file created in the backup procedure.

RAMP Customization for Docker Daemon

In this section:

- [Overview](#)
- [Pre-RAMP Installation](#)
- [Deploy RAMP on an IPv6 Setup](#)
- [Post Ramp Installation](#)

Overview

The Docker Daemon handles all the containers, volumes, and network operations for the Ribbon Application Management Platform (RAMP). The Docker containers deploy and manage the Action, EdgeView, and Object Store services.

While adding these services, the Docker creates internal networks, sometimes creating conflicts with the existing network. The default IP network for the Docker bridge is 172.17.0.0/16. To avoid such disputes, specify the networks that a Docker daemon can use and perform the following procedure:

Pre-RAMP Installation

Perform this procedure to customize the Docker networks before installing RAMP:

Start

1. Choose an option based upon your deployment:
 - a. For the VMware/KVM, uncomment the `dockerNetworkFiles` part under the write-files section of the user-data file.
 - b. For the OpenStack, uncomment the `dockerNetworkFiles` part under the write-files section of the RAMP heat template YAML file.

Note

Do not change the variable names.

Note

Docker internal network customization does not currently support IPv6.

2. Add up to seven entries for the address pools. If less than seven entries are provided, ensure the address pool generates at least seven different networks.
 You can calculate the number of networks that a single address pool can spawn using $2^{(\text{size}-\text{base})}$. For example, using base 172.27.0.0/16 with size 24 can spawn 255 Docker networks with a single entry of the address pool.

Note

The default address pool size is 24. You can select a size to facilitate spawning multiple Docker networks with a single address pool. The size must be greater than 28 and lesser than or equal to the base.

Note

The script logs an error if the provided configuration cannot generate seven Docker networks and the `daemon.json` file creation is skipped.

Openstack heat template example

```
heat_template_version: 2013-05-23
description: |
  Deploy RAMP instance.

# These are the instructions to be followed before using this template.
# If provider network is used then please select FloatingIPCount as 0
# If FloatingIPCount is 1 then it is mandatory to enter the ExternalNetworkId
# For IPv6 setup please select FloatingIPCount as 0
# For IPv6 setup please search for SEC-GROUP-V4 and comment the line below it.
# For IPv4 setup please search for SEC-GROUP-V6 and comment the line below it.
```



```
# To specify AvailabilityZone please uncomment the parameter AvailabilityZone and
uncomment the availability_zone parameter in the ems_instance resource
# HA SETUP
# To specify VIP for HA setup uncomment VirtualFixedIP and allowed_address_pairs
# For secondary HA instance, uncomment AdminSSHKeyHA
```

```
parameters:
```

```
  #comment Image input below for cinder boot
```

```
  Image:
```

```
    type: string
```

```
    label: Image
```

```
    description: Name of the glance image
```

```
  # constraints:
```

```
  #   - custom_constraint: 'glance.image'
```

```
  Flavor:
```

```
    type: string
```

```
    label: Flavor
```

```
    description: Name of the flavor
```

```
    constraints:
```

```
      - custom_constraint: 'nova.flavor'
```

```
  IPVersion:
```

```
    type: string
```

```
    label: IP Version v4/v6
```

```
    description: IP address version
```

```
    constraints:
```

```
      - allowed_values: [V6,V4]
```

```
    default: V6
```

```
  FloatingIPCount:
```

```
    type: number
```

```
    label: Floating IP count
```

```
    description: Set as 0 if floating IP is not needed. External Network Id and LI
```

```
External Network Id must be entered if it is 1
```

```
    default: 0
```

```
    constraints:
```

```
      - range: { min: 0, max: 1 }
```

```
  # First set of port and floating ip
```

```
  ManagementNetworkId:
```

```
    type: string
```

```
    label: Management Network Id
```

```
    description: Management Network Id
```

```
    default: ""
```

```
    constraints:
```

```
      - custom_constraint: 'neutron.network'
```

```
  ManagementSubnetId:
```

```
    type: string
```

```
    label: Management Subnet Id
```

```
    description: Management Subnet Id
```

```
    default: ""
```

```
  #constraints:
```

```
  #   - custom_constraint: 'neutron.subnet'
```

```
  ManagementFixedIP:
```

```
    type: string
```

```
    label: Management Fixed IP
```

```
    description: Management Fixed IP
```

```

    default: ""
# VirtualFixedIP:
#   type: string
#   label: Virtual Fixed IP
#   description: Virtual Fixed IP (VIP)
#   default: ""
ManagementFixedIPPrefix:
  type: string
  label: Management Fixed IP Prefix
  description: Management Fixed IP Prefix
  default: "24"
ManagementGateway:
  type: string
  label: Management Gateway IP
  description: Management Gateway IP
  default: ""
ExternalNetworkId:
  type: string
  label: External Network Id
  description: External Network Id
  default: ""
#   constraints:
#     - custom_constraint: 'neutron.network'
# Second set of port and parameter group
ManagementNetworkIdLI:
  type: string
  label: LI Network Id
  description: LI Management Network Id
  default: ""
  constraints:
    - custom_constraint: 'neutron.network'
ManagementSubnetIdLI:
  type: string
  label: LI Management Subnet Id
  description: LI Management Subnet Id
  default: ""
  #constraints:
  #   - custom_constraint: 'neutron.subnet'
ManagementFixedIPLI:
  type: string
  label: LI Management Fixed IP
  description: LI Management Fixed IP
  default: ""
ManagementFixedIPPrefixLI:
  type: string
  label: LI Management Fixed IP Prefix
  description: LI Management Fixed IP Prefix
  default: "24"
ManagementGatewayLI:
  type: string
  label: LI Management Gateway IP
  description: LI Management Gateway IP
  default: ""
ExternalNetworkIdLI:

```

```

    type: string
    label: LI External Network Id
    description: LI External Network Id
    default: ""
#   constraints:
#       - custom_constraint: 'neutron.network'
VolumeId:
    description: Cinder volume id
    label: Volume Id
    type: string
DnsServers:
    type: comma_delimited_list
    label: DnsServers
    description: DNS server IP addresses separated by comma
    default: ""
NtpServers:
    type: comma_delimited_list
    label: NtpServers
    description: NTP server IP address separated by comma
    default: ""
TimeZone:
    type: string
    label: TimeZone
    description: TimeZone value
    default: "America/Chicago"
    #constraints:
    #    - custom_constraint: 'timezone'
#AvailabilityZone:
#   type: string
#   label: AvailabilityZone
#   description: The availability zone
#   default: "nova"
AdminSSHKey:
    type: string
    label: AdminSSHKey
    description: Access Server public key
    default: ""
# AdminSSHKeyHA:
#   type: string
#   label: AdminSSHKeyHA
#   description: Access Server public key from primary instance
#   default: ""
InsightSSHKey:
    type: string
    label: InsightSSHKey
    description: Access Server public key
    default: ""
AdminPassword:
    type: string
    label: AdminPassword
    description: Admin Password
    default: ""
ManagementPortName:
    description: Management Network Port Name

```

```

    label: Management Network Port Name
    type: string
  LIPort:
    description: LI Mediation Server TCP/SSL port
    label: LI Mediation Server port
    type: string
    default: 15005
  #Uncomment the below input for Cinder boot
  #BootVolumeId:
    #description: Boot Cinder volume id
    #label: Boot Volume Id
    #type: string
resources:
  cloud_config:
    type: OS::Heat::CloudConfig
    properties:
      cloud_config:
        timezone: { get_param: TimeZone }
        manage_resolv_conf: true
        resolv_conf:
          nameservers: { get_param: DnsServers }
      ntp:
        enabled: true
        ntp_client: chrony
        config:
          conffpath: /etc/chrony.conf
          check_exe: chronyd
          packages:
            - chrony
          service_name: chronyd
          template: |
            ## template:jinja
            # My NTP Client config
            {%- if servers %}# servers
            {% endif %}
            {% for server in servers -%}
            server {{server}} iburst
            {% endfor %}
          servers: { get_param: NtpServers }
      users:
        - name: "insight"
          ssh_pwauth: False
          lock_passwd: False
          ssh_authorized_keys: { get_param: InsightSSHKey }

        - name: "admin"
          ssh_authorized_keys:
            - { get_param: AdminSSHKey }
            - { get_param: AdminSSHKeyHA }
#
      runcmd:
        - str_replace:
            template: usermod -p '$PASS' admin
            params:
              $PASS: { get_param: AdminPassword }

```

```
# Writing JSON user data to /opt/rbbn/userData.json
#"EnableFips" : flag for enabling/disabling FIPS during launch, By default it will be
disabled
#"EnableStig" : flag for enabling/disabling default STIGS , By default it will be
enabled.
#"stigIDs" : variable for specifying the application impacting STIGS, By default its an
empty array.
#STIG IDs in the below example can be enabled using this variable.
# eg "stigIDs" : ["V230313","V230344","V237643","V230489"]
```

```
write_files:
- path: /opt/rbbn/userData.json
  permissions: '0644'
  content: |
    {
      "EnableFips": "N",
      "EnableStig": "Y",
      "stigIDs" : []
    }
  owner: root:root
- path: /opt/rbbn/dockerNetworksFile
  permissions: '0744'
  owner: root:root
  content: |
    dockerNetwork1=172.21.0.0/16
    dockerNetworkSize1=24
    dockerNetwork2=172.22.0.0/16
    dockerNetworkSize2=24
    dockerNetwork3=172.23.0.0/16
    dockerNetworkSize3=24
    dockerNetwork4=172.24.0.0/16
    dockerNetworkSize4=24
    dockerNetwork5=172.25.0.0/16
    dockerNetworkSize5=24
    dockerNetwork6=172.26.0.0/16
    dockerNetworkSize6=24
    dockerNetwork7=172.27.0.0/16
    dockerNetworkSize7=24
```

```
cloud_init_userdata:
  type: OS::Heat::MultipartMime
  properties:
    parts:
      - config: {get_resource: cloud_config}
```

```
ems_instance:
  type: OS::Nova::Server
  properties:
    name: { get_param: "OS::stack_name" }
    #Comment the below line for cinder boot
    image: { get_param: Image }
    #Uncomment the below line for Cinder boot
```

```

    #block_device_mapping_v2: [{ device_name: "vda", volume_id : { get_param :
BootVolumeId }, delete_on_termination : "false" }]
    flavor: { get_param: Flavor }
    networks:
      - port: { get_resource: management_port }
      - port: { get_resource: management_port_li }
    user_data_format: RAW
    user_data:
      get_resource: cloud_init_userdata
    config_drive: True
    #availability_zone: { get_param: AvailabilityZone }
    metadata:
      InstanceName: { get_param: "OS::stack_name" }
      FloatingIPCountMgt: { get_param: FloatingIPCount }
    # LIFloatingIP: { get_attr: [ management_floating_ip_li, floating_ip_address, 0 ]
  }

  IF1:
    str_replace:
      template: |
        { "GW$IP_VERSION": "$GW_IP","Port": "eth0","IP$IP_VERSION": "$FIXED_IP/
$PREFIX","FIP$IP_VERSION": "$FLOATING_IP" }
      params:
        $GW_IP: {get_param: ManagementGateway}
        $FIXED_IP: {get_param: ManagementFixedIP}
        $PREFIX: {get_param: ManagementFixedIPPrefix}
        $IP_VERSION: {get_param: IPVersion }
        $FLOATING_IP: { get_attr: [ management_floating_ip, floating_ip_address,
0 ] }

  IF2:
    str_replace:
      template: |
        { "GW$IP_VERSION": "$GW_IP","Port": "eth1","IP$IP_VERSION": "$FIXED_IP/
$PREFIX","FIP$IP_VERSION": "$FLOATING_IP" }
      params:
        $GW_IP: {get_param: ManagementGatewayLI}
        $FIXED_IP: {get_param: ManagementFixedIPLI}
        $PREFIX: {get_param: ManagementFixedIPPrefixLI}
        $IP_VERSION: {get_param: IPVersion }
        $FLOATING_IP: { get_attr: [ management_floating_ip_li,
floating_ip_address, 0 ] }
    management_port:
      type: OS::Neutron::Port
      properties:
        network_id: { get_param: ManagementNetworkId }
        fixed_ips: [ { ip_address: {get_param: ManagementFixedIP} ,subnet: {get_param:
ManagementSubnetId} } ]
        name: { list_join: ["_",[ { get_param: ManagementPortName }, "1"]] }
        security_groups:
          #SEC-GROUP-V4
          #Comment out the below line for IPv6 only setup
          - { get_resource: management_security_groupv4 }
          #SEC-GROUP-V6
          #Comment out the below line for IPv4 only setup
          - { get_resource: management_security_groupv6 }

```

```

#     allowed_address_pairs: [ { ip_address: {get_param: VirtualFixedIP} } ]
management_floating_ip:
  type: "OS::Heat::ResourceGroup"
  depends_on: management_port
  deletion_policy: Retain
  properties:
    count: { get_param: FloatingIPCount }
    resource_def:
      type: OS::Neutron::FloatingIP
      properties:
        floating_network: { get_param: ExternalNetworkId }
        port_id: { get_resource: management_port }
        fixed_ip_address: { get_attr: [management_port, fixed_ips, 1, ip_address] }
        #floating_network: { get_param: ExternalNetworkId }
        #port_id: { get_resource: management_port }
# Floating IP for LI
management_port_li:
  type: OS::Neutron::Port
  properties:
    network_id: { get_param: ManagementNetworkIdLI }
    fixed_ips: [ { ip_address: {get_param: ManagementFixedIPLI} ,subnet: {get_param:
ManagementSubnetIdLI} } ]
    name: { list_join: ["_",[ { get_param: ManagementPortName },"2"]] }
    security_groups:
      #SEC-GROUP-V4
      #Comment out the below line for IPv6 only setup
      - { get_resource: li_security_groupv4 }
      #SEC-GROUP-V6
      #Comment out the below line for IPv4 only setup
      - { get_resource: li_security_groupv6 }
management_floating_ip_li:
  type: "OS::Heat::ResourceGroup"
  depends_on: management_port_li
  deletion_policy: Retain
  properties:
    count: { get_param: FloatingIPCount }
    resource_def:
      type: OS::Neutron::FloatingIP
      properties:
        floating_network: { get_param: ExternalNetworkIdLI }
        port_id: { get_resource: management_port_li }
        fixed_ip_address: { get_attr: [management_port_li, fixed_ips, 1, ip_address] }
volume_attachment:
  type: OS::Cinder::VolumeAttachment
  properties:
    volume_id: { get_param: VolumeId }
    instance_uuid: { get_resource: ems_instance }
    mountpoint: /dev/vdc
management_security_groupv4:
  type: OS::Neutron::SecurityGroup
  properties:
    description: "RAMP Management v4 Security Policy"
    name: {list_join: [' ', [ "EMS-SEC_GRP-V4-" , {get_param: "OS::stack_name"} ]]}
    rules: [

```

```

    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, protocol: ICMP, ethertype:
IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 22,
port_range_max: 22, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 123,
port_range_max: 123, protocol: UDP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 161,
port_range_max: 162, protocol: UDP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 443,
port_range_max: 443, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 5432,
port_range_max: 5432, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 6432,
port_range_max: 6432, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 6462,
port_range_max: 6462, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 1812,
port_range_max: 1812, protocol: UDP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 5200,
port_range_max: 5200, protocol: UDP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 6700,
port_range_max: 6700, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 6900,
port_range_max: 6900, protocol: UDP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 8122,
port_range_max: 8122, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 9000,
port_range_max: 9000, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 9001,
port_range_max: 9001, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 9004,
port_range_max: 9004, protocol: UDP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 5671,
port_range_max: 5671, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 8022,
port_range_max: 8022, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 8444,
port_range_max: 8444, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 9092,
port_range_max: 9092, protocol: TCP, ethertype: IPv4},
    {direction: ingress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 19991,
port_range_max: 19991, protocol: TCP, ethertype: IPv4},

    {direction: egress, remote_ip_prefix: 0.0.0.0/0, protocol: ICMP, ethertype:
IPv4},
    {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 22,
port_range_max: 22, protocol: TCP, ethertype: IPv4},
    {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 53,
port_range_max: 53, protocol: UDP, ethertype: IPv4},
    {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 123,
port_range_max: 123, protocol: UDP, ethertype: IPv4},
    {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 161,
port_range_max: 162, protocol: UDP, ethertype: IPv4},

```



```

        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 443,
port_range_max: 444, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 514,
port_range_max: 514, protocol: UDP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 514,
port_range_max: 514, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 1521,
port_range_max: 1521, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 5432,
port_range_max: 5432, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 6432,
port_range_max: 6432, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 1812,
port_range_max: 1812, protocol: UDP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 1813,
port_range_max: 1813, protocol: UDP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 2022,
port_range_max: 2022, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 2024,
port_range_max: 2024, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 2379,
port_range_max: 2379, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 5000,
port_range_max: 5000, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 5200,
port_range_max: 5200, protocol: UDP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 6700,
port_range_max: 6700, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 6900,
port_range_max: 6900, protocol: UDP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 8890,
port_range_max: 8890, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 9004,
port_range_max: 9004, protocol: UDP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 19991,
port_range_max: 19991, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 6462,
port_range_max: 6462, protocol: TCP, ethertype: IPv4},
        {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: 9092,
port_range_max: 9092, protocol: TCP, ethertype: IPv4}

    ]
management_security_groupv6:
  type: OS::Neutron::SecurityGroup
  properties:
    description: "RAMP Management v6 Security Policy"
    name: {list_join: [' ', [ "EMS-SEC_GRP-V6-" , {get_param: "OS::stack_name"} ]]}
    rules: [
      {direction: ingress, remote_ip_prefix: "::/0", protocol: ICMP, ethertype: IPv6},
      {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 22,
port_range_max: 22, protocol: TCP, ethertype: IPv6},
      {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 123,
port_range_max: 123, protocol: UDP, ethertype: IPv6},

```

```

        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 161,
port_range_max: 162, protocol: UDP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 443,
port_range_max: 443, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 5432,
port_range_max: 5432, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 6432,
port_range_max: 6432, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 6462,
port_range_max: 6462, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 1812,
port_range_max: 1812, protocol: UDP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 5200,
port_range_max: 5200, protocol: UDP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 8122,
port_range_max: 8122, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 6700,
port_range_max: 6700, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 6900,
port_range_max: 6900, protocol: UDP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 9000,
port_range_max: 9000, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 9001,
port_range_max: 9001, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 9004,
port_range_max: 9004, protocol: UDP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 9092,
port_range_max: 9092, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 5671,
port_range_max: 5671, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 8022,
port_range_max: 8022, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 8444,
port_range_max: 8444, protocol: TCP, ethertype: IPv6},
        {direction: ingress, remote_ip_prefix: "::/0", port_range_min: 19991,
port_range_max: 19991, protocol: TCP, ethertype: IPv6},

        {direction: egress, remote_ip_prefix: "::/0", protocol: ICMP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 22,
port_range_max: 22, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 53,
port_range_max: 53, protocol: UDP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 123,
port_range_max: 123, protocol: UDP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 161,
port_range_max: 162, protocol: UDP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 443,
port_range_max: 444, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 514,
port_range_max: 514, protocol: UDP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 514,
port_range_max: 514, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 1521,
port_range_max: 1521, protocol: TCP, ethertype: IPv6},

```

```

        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 5432,
port_range_max: 5432, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 6432,
port_range_max: 6432, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 1812,
port_range_max: 1812, protocol: UDP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 1813,
port_range_max: 1813, protocol: UDP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 2022,
port_range_max: 2022, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 2024,
port_range_max: 2024, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 2379,
port_range_max: 2379, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 5000,
port_range_max: 5000, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 5200,
port_range_max: 5200, protocol: UDP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 6700,
port_range_max: 6700, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 6900,
port_range_max: 6900, protocol: UDP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 8890,
port_range_max: 8890, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 9004,
port_range_max: 9004, protocol: UDP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 19991,
port_range_max: 19991, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 6462,
port_range_max: 6462, protocol: TCP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: 9092,
port_range_max: 9092, protocol: TCP, ethertype: IPv6}
    ]

    li_security_groupv4:
      type: OS::Neutron::SecurityGroup
      properties:
        description: "RAMP LI v4 Security Policy"
        name: {list_join: [' ', [ "EMS-SEC_GRP-LI-V4-" , {get_param: "OS::stack_name"} ]]}
        rules: [
          {direction: ingress, remote_ip_prefix: 0.0.0.0/0, protocol: ICMP, ethertype:
IPv4},
          {direction: egress, remote_ip_prefix: 0.0.0.0/0, protocol: ICMP, ethertype:
IPv4},
          {direction: egress, remote_ip_prefix: 0.0.0.0/0, port_range_min: {get_param:
LIPort}, port_range_max: {get_param: LIPort}, protocol: TCP, ethertype: IPv4}
        ]

    li_security_groupv6:
      type: OS::Neutron::SecurityGroup
      properties:
        description: "RAMP LI v6 Security Policy"
        name: {list_join: [' ', [ "EMS-SEC_GRP-LI-V6-" , {get_param: "OS::stack_name"} ]]}
        rules: [

```

```

        {direction: ingress, remote_ip_prefix: "::/0", protocol: ICMP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", protocol: ICMP, ethertype: IPv6},
        {direction: egress, remote_ip_prefix: "::/0", port_range_min: {get_param:
LIPort},    port_range_max: {get_param: LIPort},    protocol: TCP, ethertype: IPv6}
    ]

outputs:
  management_floating_ip:
    description: Floating IP address of ems_instance in external network
    value: { get_attr: [ management_floating_ip, floating_ip_address ] }

```

VMware/KVM user-data file example

```

#cloud-config
timezone: "Asia/Kolkata"
ntp:
  enabled: true
  ntp_client: chrony
  config:
    confpath: /etc/chrony.conf
    check_exe: chronyd
    packages:
      - chrony
    service_name: chronyd
    template: |
      ## template:jinja
      # My NTP Client config
      {%- if servers %}# servers
      {% endif %}
      {% for server in servers -%}
      server {{server}} iburst
      {% endfor %}
  servers:
    - 10.128.254.68
manage_resolv_conf: true
resolv_conf:
  nameservers: ['$dnsServer']
  searchdomains:
    - $dnsSearchPath
write_files:
  - path: /opt/rbbn/userData.json
    permissions: '0644'
    content: |
      {
        "IF1": {"GWV4": "10.11.14.1", "IPV4": "10.11.15.153/23","Port": "eth0"},
        "IF2": {"GWV4": "", "IPV4": "/", "Port": ""},
        "growpart": { "opt" : 60, "pgsql": 30, "home":10},
        "InstanceName": "VinayRamp"
      }
    owner: root:root
  - path: /opt/rbbn/dockerNetworksFile

```

```
permissions: '0777'
content: |
  dockerNetwork1=172.21.0.0/16
  dockerNetworkSize1=24
  dockerNetwork2=172.22.0.0/16
  dockerNetworkSize2=24
  dockerNetwork3=172.23.0.0/16
  dockerNetworkSize3=24
  dockerNetwork4=172.24.0.0/16
  dockerNetworkSize4=24
  dockerNetwork5=172.25.0.0/16
  dockerNetworkSize5=24
  dockerNetwork6=172.26.0.0/16
  dockerNetworkSize6=24
  dockerNetwork7=172.27.0.0/16
  dockerNetworkSize7=24
owner: root:root
runcmd:
  - usermod -p '$1$admin$1kgWpnZpUx.vTroWPXPIB0' admin
  - usermod -f -1 admin
```

Deploy RAMP on an IPv6 Setup

Perform this procedure to deploy the RAMP on an IPv6 setup:

Start

1. Create or edit the `/etc/docker/daemon.json` file using:

```
{
  "experimental": true,
  "ipv6": true,
  "ip6tables": true,
  "fixed-cidr-v6": "fd00:10:6b51:6200::/64",
}
```

2. Restart the Docker service after changing the `daemon.json` file.

```
systemctl stop docker.service
systemctl start docker.service
```

Post Ramp Installation

Perform this procedure to customize the Docker networks after installing RAMP:

1. Disable the health check for EV/ACS/OSS:
 - a. Switch to `root` user:

```
sudo su
/opt/sonus/ems/conf/manage0saf.sh
```

- b. Select the `disable Healthcheck` option.
- c. Select the `EV/ Action Service/ Object store service` option.

2. Call `stop` scripts of EV/ACS/OSS.

```
su - insight
/opt/oss-build/oss_actionscript stop (only if OSS is installed on RAMP)
/opt/acs-build/acs_actionscript stop (only if ACS is installed on RAMP)
/opt/sonus/ems/conf/opensaf/AS/edgeview_actionscript stop (only if EV is installed
on RAMP)
```

3. You can calculate the number of networks that a single address pool can spawn using $2^{(\text{size}-\text{base})}$. For example, using base 172.27.0.0/16 with size 24 can spawn 255 Docker networks with a single entry of the address pool.

You can select a size to facilitate spawning multiple Docker networks with a single address pool. The size must be greater than 28 and lesser than or equal to the base.

4. As `root` user, modify or create: `/etc/docker/daemon.json`

Example:

```
{
  "default-address-pools": [
    {
      "base": "172.27.0.0/16",
      "size": 24
    },
    {
      "base": "172.28.0.0/16",
      "size": 24
    },
    {
      "base": "172.29.0.0/16",
      "size": 24
    },
    {
      "base": "172.30.0.0/16",
      "size": 24
    },
    {
      "base": "172.31.0.0/16",
```

```

    "size": 24
  },
  {
    "base": "172.32.0.0/16",
    "size": 24
  },
  {
    "base": "172.26.0.0/16",
    "size": 24
  }
]
}
```

5. Restart docker service:

```
systemctl stop docker
systemctl start docker
```

6. Call `start` scripts of EV/ACS/OSS.

```
su - insight
/opt/acs-build/acs_actionscript start (only if ACS is installed on RAMP)
/opt/sonus/ems/conf/opensaf/AS/edgeview_actionscript start (only if EV is
installed on RAMP)
/opt/oss-build/oss_actionscript start (only if OSS is installed on RAMP)
```

7. Enable the Healthcheck for ACS/EV/OSS:
 - a. Exit from `insight` user and switch to the `root` user:

```
sudo su
/opt/sonus/ems/conf/manage0saf.sh
```

- b. Select the option `enable Healthcheck`.
 - c. Select the option `(EV/ Action Service/ Object store service)`.

You may face issue for launching bulk actions on EdgeMarc devices for few mins, but this issue should get resolved in 10 minutes.

Upgrading RAMP

Contents

- [Pre-Upgrade Checklist](#)
- [Upgrading RAMP in Virtual and Private Cloud Environments](#)
 - [Upgrading RAMP on KVM](#)
 - [Upgrading RAMP on OpenStack](#)
 - [Upgrading RAMP on VMware](#)
- [Upgrading RAMP in Public Cloud Environments](#)
 - [Upgrading RAMP on AWS](#)
 - [Upgrading RAMP on Azure](#)
- [Upgrading RAMP CNF](#)
 - [RAMP CNF - Pre-Upgrade Checklist](#)
 - [RAMP CNF - Upgrade Standalone Instance Using Helm Commands](#)
 - [RAMP CNF - Upgrade RAMP GR Instance Using Helm Commands](#)
 - [RAMP CNF - Upgrade Standalone Instance Using GIT](#)
 - [RAMP CNF - Upgrade RAMP GR Instance Using GIT](#)
 - [RAMP CNF - Post-Upgrade Procedures](#)
- [Post-Upgrade Procedures for RAMP](#)
 - [Clear the Client Java Cache and Browser Cookies After Upgrade](#)

Pre-Upgrade Checklist

Accomplish these tasks at least seven days before starting the Ribbon Application Management Platform (RAMP) upgrade:

1	Check terminal and user access 1. Check if the terminal access to the RAMP is available. 2. Check if the Insight, postgres, and root passwords are available.
2	Verify release interoperability with other Ribbon products in your network Ensure that other elements integrated with RAMP are compatible with the target RAMP release according to the interoperability Matrix at: Ribbon Application Management Platform Interoperability Matrix
3	Verify Bulletins and Warnings (WBAs) 1. Review all bulletins listed under RAMP Release Information section Associated Ribbon Bulletins/Announcements. 2. Verify all Warnings/Bulletins applicable to the upgrade path in the Ribbon Support Portal.
4	Review Release Notes Review RNs for RAMP configuration requirements that may need to be in place before the upgrade. Some examples are software configuration requirements and upgrade notes under the 'Install and upgrade notes' sections.

5	Prepare software 1. Review the RN 'Software Bundle' section to identify the application software files required for the upgrade. 2. Follow the upgrade section applicable to your RAMP environment for the location of where to transfer the application files. 3. Follow Download Files from Ribbon Support Portal for instructions to obtain software and create target directories for application files on RAMP.
6	Check RAMP Status 1. Confirm all processes are running. Refer to Check RAMP Status. 2. For RAMP GR, check the replication status before the upgrade. Refer to Check Database and File Replication Status. 3. Check whether API, CLI, PM, FM, PSX Manager, SBC Manager, and other core RAMP functions are operational. If running the EdgeView, verify the container health as an <code>Insight</code> user: <pre>cd /opt/scc-build/ docker-compose ps</pre>
7	Review Upgrade Prerequisites Review the documentation section 'Upgrade prerequisites' or 'Prerequisites' depending on the RAMP environment. For more information, refer to Checklist for Installing RAMP on OpenStack, Check KVM Host System Requirements or Checklist for Installing RAMP on VMware.
8	Remove Files and Folders Ensure the following files and folders are removed: • <code>/opt/rbbn/lm/migrate/export/data</code> • <code>/opt/rbbn/lm/migrate/sql</code> • <code>/opt/devMgmt/data/migrate/sql/importData.sql</code> • <code>/opt/devMgmt/backup/devMgmtDataBackup.tar</code>
9	Check Hostname 1. Check whether the RAMP hostname matches installation requirements. 2. Hostname value using the hostname command must match values on <code>/etc/hosts</code> and <code>/etc/sysconfig/network</code> configuration files. 3. The hostname configuration is case-sensitive. 4. For Hostname/Instance name conventions, refer to Hostname and Instance Name Conventions.

10 Check managed elements

Verify communication between RAMP and the managed elements. Find the nodes for which the RAMP discovery failed.

1. Open the file `/opt/devMgmt/logs/reachability_audit_log`.
2. Search for the string "timeout".

Example:

```
62023-06-19 18:31:16,875 IST INFO [Reachability_Worker-38]
NotificationManager - localhost, SNMP, 10.54.141.91, 161, 5, RESPONSE
```

timeout, <reachability count>, <node name>, <IP address of the node>

3. Rediscover the non-cloud nodes for which RAMP discovery failed.

Upgrading RAMP in Virtual and Private Cloud Environments

In this section:

- [Upgrading RAMP on KVM](#)
 - [Create a Dump File of RAMP on KVM](#)
 - [Upgrade RAMP Standalone on KVM](#)
 - [Upgrade RAMP GR on KVM](#)
 - [Revert RAMP Upgrade on KVM](#)
- [Upgrading RAMP on OpenStack](#)
 - [Upgrade RAMP Standalone on OpenStack](#)
 - [Upgrade RAMP GR on OpenStack](#)
 - [Roll Back RAMP GR for Upgrade Failure](#)
- [Upgrading RAMP on VMware](#)
 - [Upgrade RAMP Standalone on VMware](#)
 - [Take a Snapshot of RAMP on VMware](#)
 - [Upgrade RAMP GR on VMware](#)
 - [Revert RAMP Upgrade on VMware](#)

Upgrading RAMP on KVM

To upgrade the Ribbon Application Management Platform (RAMP) perform the procedures outlined in the following sections:

In this section:

- [Create a Dump File of RAMP on KVM](#)
- [Upgrade RAMP Standalone on KVM](#)
- [Upgrade RAMP GR on KVM](#)
- [Revert RAMP Upgrade on KVM](#)

Create a Dump File of RAMP on KVM

You can create a dump file (backup) of a Ribbon Application Management Platform (RAMP) instance on KVM to store information for its current state. If an upgrade fails or requires reverting, the dump file is needed to restore the previous version of RAMP.

To create the dump file:

Start

1. SSH to the KVM host as the `root` user.
2. Create the RAMP dump file using the following command:

```
virsh dumpxml name_of_the_instance >  
Path_InstanceDump_name_of_the_instance_Revert.xml
```

Example output file for a RAMP instance

```
virsh dumpxml rampInstance > /home/backup/rampInstance_Revert.xml
```

A dump file of this type is required to revert an upgrade.

Upgrade RAMP Standalone on KVM

Related articles:

- [Take a Backup of RAMP for Upgrade](#)
- [Installing RAMP on KVM Manually](#)
- [Restore from Backup on RAMP Standalone](#)
- [Create a Dump File of RAMP on KVM](#)
- [Revert RAMP Upgrade on KVM](#)
- [Post-Upgrade Procedures for RAMP](#)

Use the following procedure to upgrade a standalone instance of Ribbon Application Management Platform (RAMP) on KVM (Kernel Virtual Machine). During this procedure, you backup your current database and application and copy it into a new instance with the latest version of RAMP software installed.

Prerequisites

A host is available to store the backup.

Start

1. Log on to RAMP as the `admin` user.
2. Switch to `root` user:

```
sudo su -
```

3. (Optional) If you manage SBC Edge devices using RAMP, complete the following steps to back up the EdgeView (EV) database:

Note

This step is needed only for pre 22.06 RAMP.

- a. Download the `rampBootstrap-V <version> .tar` file for the RAMP version you are upgrading.
- b. Extract the `rampBootstrap-V <version> .tar` file:

```
tar -xvf rampBootstrap-V<version>.tar
```

where <version> is the RAMP version to which you are upgrading.

- c. Change to the `/opt/sonus/ems/conf` directory and take a backup copy of the `edge_view_config` file.
- d. From the files extracted from the `rampBootstrap-V <version> .tar` file, copy the `edge-view-config` file to the `/opt/sonus/ems/conf` directory.
4. Take a backup of the RAMP database and copy it to a remote server. For more information, refer to [Take a Backup of RAMP for Upgrade](#).
5. Log into the KVM host.
6. If you want to upgrade the device after a RAMP upgrade, the uploaded SBC image file `SBC.gz` is not restored as part of the upgrade. (Optional) If you need the image files, copy the contents of `/opt/sonus/ems/image_upgrade` to a third-party server:

```
scp -r /opt/sonus/ems/image_upgrade/* admin@<remote_ip>:/opt/sbc_image_bkup/
```

7. (Optional) Create a dump file of the RAMP instance to use if you need to revert to the prior version of RAMP. If the source RAMP version is 22.12 and onwards, refer to [Create a Dump File of RAMP on KVM](#).

Note

The remaining upgrade steps are service-impacting.

8. Delete the RAMP instance:

```
virsh destroy <name of the instance>
virsh undefine <name of the instance>
```

9. Instantiate an instance of RAMP using the latest version of software. For more information, refer to [Installing RAMP on KVM Manually](#).
10. (Optional) If you manage SBC Edge devices with RAMP and you backed up the EV database:

```
/opt/sonus/ems/conf/edge_view_config add
```

For more information, refer to [Deploy Optional Services on RAMP](#).

11. Restore the RAMP. For more information, refer to [Restore from Backup on RAMP Standalone](#).
12. Perform post-upgrade procedures. For more information, refer to [Post-Upgrade Procedures for RAMP](#).

Upgrade RAMP GR on KVM

Related articles:

- [Tear Down RAMP GR](#)
- [Restore from Backup on RAMP Standalone](#)
- [Installing RAMP on KVM Manually](#)
- [Configuring RAMP GR](#)
- [Revert RAMP Upgrade on KVM](#)

Use the following procedure to upgrade a geographically redundant (GR) pair of Ribbon Application Management Platform (RAMP) instances on KVM (Kernel Virtual Machine). A RAMP GR deployment consists of an active (source) and standby (target) pair of instances. During this procedure, you will back up your current database and copy it to new instances with the current version of the RAMP software installed.

Prerequisites

- A host is available to store the backup.
- Ribbon recommends stopping RAMP before taking a backup.

Start

1. Copy the `insight` and `admin` user SSH keys to a secure, external location for both the active and standby RAMP instances:
 - To obtain the SSH keys for the `insight` user, complete the procedure on [Obtain the RAMP SSH Keys](#).
 - To obtain the SSH keys for the `admin` user, repeat the same procedure, except for the `admin` keys, SSH to the RAMP IP address as the `admin` user (instead of the `insight` user):

```
ssh admin@10.14.55.120
```

2. Log on to the KVM host.

Note

The remaining upgrade steps are service-impacting. Do not configure anything during the upgrade, as data may be lost.

3. Tear down the RAMP GR configuration to separate the instances. Refer to [Tear Down RAMP GR](#).
4. Upgrade the configured active RAMP instance. Refer to [Upgrade RAMP Standalone on KVM](#).

5. Perform the following to delete the standby RAMP instance and create a new RAMP instance using the latest version:
 - a. Log on to the KVM host.
 - b. (Optional) Create a dump file of the RAMP instance to use if you need to revert to the prior version of RAMP. If the source RAMP version is 22.12 and above, refer to [Create a Dump File of RAMP on KVM](#).
 - c. Delete the standby RAMP instance:

```
virsh destroy <name of the instance>
virsh undefine <name of the instance>
```

- d. Instantiate an instance of the standby RAMP using the latest software version. For more information, refer to [Installing RAMP on KVM Manually](#).
- e. (Optional) If you manage SBC Edge devices using RAMP and backed up, then deploy the optional services on RAMP. For more information, refer to [Deploy Optional Services on RAMP](#).
6. (Optional) In the case of an auto switchover enabled RAMP, you can upgrade the ETCD VMs to the latest available or released version. For more information, refer to [Upgrading etcd](#). Refer to the software bundles section of the latest release notes [RAMP Release Information](#).
7. Complete GR configuration for the pair of RAMP instances, using the configured active as the active instance. Refer to [Configuring RAMP GR](#).
8. Perform post-upgrade procedures on the active RAMP instance. Refer to [Post-Upgrade Procedures for RAMP](#).

Revert RAMP Upgrade on KVM

If you [created a dump file](#) of your Ribbon Application Management Platform (RAMP) instance prior to upgrade, you can use the dump file for the instance to revert to your prior version of RAMP, if necessary.

Manually remove the latest QCOW2 file and its config drive if they were associated with a failed upgrade.

To revert RAMP on KVM:

1. Shut down the RAMP instance:

```
virsh destroy <instance-Name>
```

Example

```
virsh destroy ramp-vmconf-nk
```

2. Undefine the resources attached to the instance:

```
virsh undefine <instance-Name>
```

Example

```
virsh undefine ramp-vmconf-nk
```

3. Define the instance using the revert XML dump file you created during upgrade:

```
virsh define <Path>/InstanceDump-<instance-Name>-Revert.xml
```

The following is an example of defining the instance using the instance dump file: `/home/InstanceDumpBackUP/InstanceDump-ems-vmconf-nk-Revert.xml`

Example

```
virsh define /home/InstanceDumpBackUP/InstanceDump-ramp-vmconf-nk-Revert.xml
```

4. Start the instance:

```
virsh start <instance-Name>
```

Example

```
virsh start ramp-vmconf-nk
```

Upgrading RAMP on OpenStack

To upgrade the Ribbon Application Management Platform (RAMP) perform the procedures outlined in the following sections:

In this section:

- [Upgrade RAMP Standalone on OpenStack](#)
- [Upgrade RAMP GR on OpenStack](#)
- [Roll Back RAMP GR for Upgrade Failure](#)

Upgrade RAMP Standalone on OpenStack

- [Prerequisites](#)
- [Backup Procedures](#)
- [Upgrade Procedure](#)

Use the following procedure to upgrade a standalone Ribbon Application Management Platform (RAMP) instance on OpenStack. Before upgrading, you will back up data from your existing RAMP instance. To upgrade, you will first delete the existing stack for the instance. You will then create a new instance using the current version of RAMP software and with the existing Cinder volume attached.

Prerequisites

- Make Ensure you know the passwords for all default RAMP accounts.
- Make a note of the licenses available on your system so you can verify the list after the upgrade. Refer to [License Management](#) for information on viewing licenses.

Backup Procedures

Step	Action
1	Make a copy of the stack parameters for your current deployment on OpenStack to ensure that the values are available when you launch the new instance. 1. Log onto the OpenStack Dashboard GUI. 2. Click Project > Orchestration > Stacks > Select the Source Stack > Overview. The Overview tab opens. 3. Record the values for the following parameters: - OracleSSHKey - LIPort - TimeZone - ManagementFixedIPLI - ManagementSubnetIdLI - ManagementSubnetId - NtpServers - FloatingIPCount - ExternalNetworkId - ManagementGateway - ManagementNetworkId - InsightSSHKey - ManagementFixedIPPrefixLI - ManagementFixedIPPrefix - OS::stack_name - ManagementNetworkIdLI - ManagementFixedIP - IPVersion - DnsServers - ExternalNetworkIdLI - AdminPassword - AdminSSHKey - VolumId - ManagementPortName - Flavor - ManagementGatewayLI
2	Take a back up of the RAMP instance and copy it to a remote system. Refer to Take a Backup of RAMP for Daily Maintenance. Taking a system backup is essential so that you have backup data available to restore the system if the upgrade fails.
3	Export performance management data from the RAMP instance to an external server. Refer to Collect and Export Device Statistics.
4	Copy the RAMP active SSH keys, <code>authorized_keys</code>, and <code>known_hosts</code> for the insight user to a remote server. Refer to Obtain the RAMP SSH Keys.

The Action service is an optional service from the RAMP 24.03R1 onwards. During an upgrade, the Action service is enabled by default, only when the Action and EdgeView services are enabled in previous releases. If only the action service is enabled in the previous release, then the upgrade action service is not enabled by default.

Upgrade Procedure

Step	Action
1	Create a Glance Image for the new RAMP version. Refer to Create a Glance Image .
2	Complete the following to delete the existing stack of the Ribbon Application Management Platform (RAMP) instance and create a new RAMP instance with the existing volume: - Using the OpenStack Dashboard GUI, shut off the RAMP instance: - Navigate to Project > Instances. - Select the RAMP instance from the drop-down menu. - Select Shut off instance. - Delete the stack of the RAMP instance. Refer to Delete Stack. - Instantiate a RAMP instance with the following: - identical stack name and hostname Note For information on hostnames, refer to Hostname and Instance Name Conventions. The SSH keys for the admin and insight users are restored only if the hostname matches. The hostname is case-sensitive. - The IP address of the deleted RAMP instance - existing Cinder volume - new Glance image and Heat template for the current version of RAMP software. Refer to Instantiate RAMP on OpenStack.
3	Check the status of the RAMP node. Refer to Check RAMP Status. Ensure that the RAMP node is running before proceeding.

Step	Action
4	Check whether the SSH keys, <code>authorized_keys</code>, and <code>known_hosts</code> for the insight user on the RAMP node are the same as the entries you recorded before the upgrade. Note When restoring the database, these files are replaced with the backup files from the RAMP Cinder volume.
5	Perform post-upgrade procedures. Refer to Post-Upgrade Procedures for RAMP .
6	Reboot the SBC and PSX nodes managed on RAMP. • If any of the SBC or PSX nodes fail during the upgrade, you can instantiate new nodes using the same IP address. • The new node will come up with the same configuration by reusing the IP address in the same cluster. These nodes will register and their passwords will be available on the upgraded RAMP instance.

Upgrade RAMP GR on OpenStack

Use the following procedure to upgrade a pair of geographically redundant (GR) instances of the Ribbon Application Management Platform (RAMP) on OpenStack. Before upgrading, back up data from your existing RAMP instances. To upgrade, first delete the existing stack for the instance. Next, create new instances using the current version of RAMP software and the existing attached Cinder volumes. Once the new instances are instantiated, configure them for GR.

Prerequisites

- Ensure you know the passwords for all default RAMP accounts.
- Make a note of the licenses available on your system so you can verify the list after the upgrade. For more information on viewing licenses, refer to [License Management](#).
- Check the database and file replication status on the GR deployment to ensure that synchronization is current. For more information, refer to [Check Database and File Replication Status](#).

Back up Procedure

Step	Action
1	Make a copy of the stack parameters for both the active and standby instances in your current deployment on OpenStack to ensure that you have the values available when you launch the new instances. 1. Log on to the OpenStack Dashboard GUI. 2. Click Project > Orchestration > Stacks > Select the Source Stack > Overview. The Overview tab opens. 3. Record the values for the following parameters: - OracleSSHKey - LIPort - TimeZone - ManagementFixedIPLI - ManagementSubnetIdLI - ManagementSubnetId - NtpServers - FloatingIPCount - ExternalNetworkId - ManagementGateway - ManagementNetworkId - InsightSSHKey - ManagementFixedIPPrefixLI - ManagementFixedIPPrefix - OS::stack_name - ManagementNetworkIdLI - ManagementFixedIP - IPVersion - DnsServers - ExternalNetworkIdLI - AdminPassword - AdminSSHKey - VolumId - ManagementPortName - Flavor - ManagementGatewayLI
2	Take a backup of the RAMP active instance and copy it to a remote system. For more information, refer to Take a Backup of RAMP for Daily Maintenance. A system backup is essential so that you have backup data available to restore the system if the upgrade fails.
3	Export performance management data from the RAMP active instance to an external server. For more information, refer to Collect and Export Device Statistics.
4	Copy the RAMP SSH keys, <code>authorized_keys</code>, and <code>known_hosts</code> for the insight user on both the active and standby instances to a remote server. For more information, refer to Obtain the RAMP SSH Keys.

Step	Action
5	Remove all the registered C3 G9EMS devices from the RAMP if upgraded from pre-V24.06.

Upgrade Procedure

S t e p	Action
1	Create a Glance Image for the new RAMP version. For more information, refer to Create a Glance Image .
2	Tear down the GR configuration. For more information, refer to Tear Down RAMP GR. After you tear down the GR configuration, database changes (including servicing the network) are no longer synced between the RAMP active and standby instances. The teardown process stops database replication and makes the RAMP active and standby instances work as standalone instances.
3	Check the status of the RAMP standby instance. For more information, refer to Check RAMP Status. Note Ensure that the RAMP standby instance is running before proceeding.
4	Stop and start the active RAMP instance. For more information, refer to How to Start and Stop RAMP. Note This is required to update the Config Store IP on the SBC nodes with the active RAMP IP.

Step	Action
5	Complete the following to delete the existing stack of the RAMP active instance and create a new RAMP instance with the existing volume. The new instance becomes the RAMP active instance. - Using the OpenStack Dashboard GUI, shut off the RAMP active instance: - Navigate to Project > Instances. - Select the RAMP active instance from the drop-down menu. - Select Shut off instance. - Delete the stack of the RAMP active instance. For more information, refer to Delete Stack. - Instantiate a RAMP instance to be the active instance with the following: - Identical stack name and hostname. Note For information on hostnames, refer to Hostname and Instance Name Conventions. The ssh keys for the admin and insight users are restored only if the hostname matches. The hostname is case sensitive. - The IP address of the deleted RAMP active instance. - Existing Cinder volume. - New Glance image and Heat template for the current version of RAMP software. For more information, refer to Instantiate RAMP on OpenStack. Note There is no loss of PM Collection data as the RAMP standby instance is running.
6	Check the status of the RAMP active instance. For more information, refer to Check RAMP Status. Note Ensure that the RAMP active instance is running before proceeding.
7	Check whether the SSH keys, <code>authorized_keys</code>, and <code>known_hosts</code> for the insight user on the RAMP active instance are the same as the entries you recorded before the upgrade. Note When restoring the database, these files are replaced with the files available in the Cinder volume.
8	Perform post-upgrade procedures on the RAMP active instance. For more information, refer to Post-Upgrade Procedures for RAMP.

Step	Action
9	Stop the RAMP standby instance. For more information, refer to How to Start and Stop RAMP. Note The RAMP active instance contains the database at this point.
10	Complete the following to delete the existing stack of the RAMP standby instance and create a new RAMP instance with the existing Cinder volume. The new instance becomes the RAMP standby instance: - Using the OpenStack Dashboard GUI, shut off the RAMP standby instance: - Navigate to Project > Instances. - Select the RAMP standby instance from the drop-down menu. - Select Shut off instance. - Delete the stack of the RAMP standby instance. For more information, refer to Delete Stack. - Instantiate a RAMP instance to be the standby instance with the following: - Identical stack name and hostname. Note For information on hostnames, refer to Hostname and Instance Name Conventions. The ssh keys for the admin and insight users are restored only if the hostname matches. The hostname is case sensitive. - The IP address of the deleted RAMP standby instance. - Existing Cinder volume. - New Glance image and Heat template for the current version of RAMP software. For more information, refer to Instantiate RAMP on OpenStack.
11	Copy the SSH key of the new RAMP active instance to the standby instance. For more information, refer to Copy SSH Keys to Instantiate a RAMP Standby Instance.
12	Check the status of the RAMP standby instance. For more information, refer to Check RAMP Status. Note Ensure that the RAMP standby instance is running before proceeding.
13	Check whether the SSH keys, <code>authorized_keys</code>, and <code>known_hosts</code> for the insight user in the RAMP standby instance are the same as before the upgrade.

Step	Action
1 4	Stop and start the active RAMP instance. For more information, refer to How to Start and Stop RAMP. Note This is required to update the Config Store IP on the SBC nodes with active RAMP IP.
1 5	(Optional) In the case of an autoswitchover enabled RAMP, you can upgrade the ETCD VMs to the latest available or released version. For more information, refer to Upgrading etcd. Refer to the software bundles section of the latest release notes RAMP Release Information.
1 6	On the RAMP active instance, configure GR parameters. For more information, refer to Configuring RAMP GR. Note There may be performance management collection data loss for around 15 minutes while configuring GR. In addition, the PM data collected by the standby RAMP instance while recreating the RAMP active instance will be lost while configuring RAMP GR. During an upgrade, data sync does not occur between the RAMP standby and active instances.
1 7	The status of the active and standby instances may show as offline on the upgraded RAMP. Rediscover both active and standby RAMP instances. For more information, refer to How to Rediscover the localhost.

Step	Action
1 8	Complete the following procedure to ensure that password-less SSH connection is working from the RAMP active to standby instance and vice versa. - Log on to the RAMP active instance as the <code>admin</code> user. - Change to the <code>insight</code> user: <pre>su - insight</pre> - Navigate to the directory: <pre>cd .ssh</pre> - SSH to the RAMP standby instance: <pre>ssh insight@<IP address of the RAMP standby instance></pre> If the SSH password-less connection is intact, you are not prompted for a password. - Log on to the RAMP standby instance as an <code>admin</code> user. - Change to the <code>insight</code> user: <pre>su - insight</pre> - Navigate to the following directory: <pre>cd .ssh</pre> - SSH to the RAMP active instance: <pre>ssh insight@<IP address of the RAMP active instance></pre> If the SSH password-less connection is intact, you are not prompted for a password.

S t e p	Action
1 9	Reboot the SBC and PSX nodes managed on RAMP. Note • If any of the SBC or PSX nodes fail during the upgrade, you can instantiate new nodes using the same IP address. • The new SBC/PSX nodes are registered on the RAMP standby instance with the same IP address. • The new node will come up with the same configuration by reusing the IP address in the same cluster. • However, passwords of the PSX/SBC nodes saved in the RAMP standby instance do not sync to the active RAMP instance. When both RAMP active and standby instances are up, and GR is configured, reboot the SBC and PSX nodes that were: • instantiated (with the same IP addresses). • rebooted during the upgrade and whose configuration is edited. These nodes register (and their passwords are available) on the RAMP active instance.

Roll Back RAMP GR for Upgrade Failure

In case of failure during upgrade of a Ribbon Application Management Platform (RAMP) geo-redundant (GR) deployment, the following table outlines steps to take to roll back your deployment depending on the point during upgrade when the failure occurred.

For cinder failure, a backup must be available to restore the backup.

Rollback Procedures Based on Upgrade Status

Upgrade status	Procedures to follow
• Tear down GR completed • RAMP active (source) instance upgraded	1. Perform the following on the RAMP active instance: a. Delete the RAMP active instance on OpenStack. b. Create a new cinder volume. Refer to Create a Cinder Volume. c. Update the environment file with the following (all the parameters must be same as the deleted instance apart from the volume Id and the image): • New cinder volume UUID. • RAMP QCOW2 image for the previous release. d. Instantiate with the updated environment file. e. Restore the backup file to the RAMP active instance. Refer to Restore from Backup on RAMP Standalone. 2. Instantiate standby (target) instance with the previous version of QCOW2 image. 3. Configure GR. Refer to Configuring RAMP GR.
• Tear down GR completed • RAMP active instance upgraded • RAMP standby instance upgraded	1. Perform the following on RAMP active and standby instances: a. Delete the RAMP active instance on Openstack. b. Create a new cinder volume. Refer to Create a Cinder Volume. c. Update the environment file with the following (all the parameters must be same as the deleted instance apart from the volume Id and the image): ◦ New cinder volume UUID. ◦ RAMP QCOW2 image for the previous release. d. Instantiate with the updated environment file. e. Restore the backup file to the RAMP instance. Refer to Restore from Backup on RAMP Standalone. 2. Configure GR. Refer to Configuring RAMP GR.
• Tear down GR completed • RAMP active instance upgraded • RAMP standby instance upgraded • GR is configured • Some features are not functional.	1. Perform the following on RAMP active and standby instances. 2. a. Delete the RAMP active instance on Openstack. b. Create a new cinder volume. Refer to Create a Cinder Volume. c. Update the environment file with the following (all the parameters must be same as the deleted instance apart from the volume Id and the image): ◦ New cinder volume UUID. ◦ RAMP QCOW2 image for the previous release. d. Instantiate with the updated environment file. e. Restore the backup file to the RAMP instance. Refer to Restore from Backup on RAMP Standalone. 3. Configure GR. Refer to Configuring RAMP GR.

Upgrading RAMP on VMware

To upgrade the Ribbon Application Management Platform (RAMP) perform the procedures outlined in the following sections:

In this section:

- [Upgrade RAMP Standalone on VMware](#)
- [Take a Snapshot of RAMP on VMware](#)
- [Upgrade RAMP GR on VMware](#)
- [Revert RAMP Upgrade on VMware](#)

Upgrade RAMP Standalone on VMware

Related articles:

- [Take a Backup of RAMP for Upgrade](#)
- [Take a Snapshot of RAMP on VMware](#)
- [Restore from Backup on RAMP Standalone](#)
- [Installing RAMP on VMware Manually](#)
- [Post-Upgrade Procedures for RAMP](#)

Use the following procedure to upgrade a standalone instance of Ribbon Application Management Platform (RAMP) on VMware. During this procedure you will take a backup of your current database and copy it into a new instance with the current version of RAMP software installed.

Prerequisites

- A host is available to store the backup.

Start

1. Log on to RAMP as the `admin` user.
2. Enter the following command to switch to the `root` user:

```
sudo su -
```

3. (Optional) If you manage SBC Edge devices with RAMP, complete the following steps to back up the EdgeView (EV) database:

Note

This step is needed only for pre 22.06 RAMP.

- a. Download the `rampBootstrap-V <version> .tar` file for the RAMP version to which you are upgrading.
- b. Extract the `rampBootstrap-V <version> .tar` file using the following command:

```
tar -xvf rampBootstrap-V <version> .tar
```

where `<version>` is the RAMP version to which you are upgrading.

- c. Change to the `/opt/sonus/ems/conf` directory and take a backup copy of the `edge_view_config` file.
- d. From the files extracted from the `rampBootstrap-V <version> .tar` file, copy the `edge-view-config` file to the `/opt/sonus/ems/conf` directory.
4. Take a backup of the RAMP database and copy it to a remote server. For more information, refer to [Take a Backup of RAMP for Upgrade](#).
5. (Optional) Take a snapshot of the RAMP VM to check if you need to revert it to the prior version of RAMP. For more information, refer to [Take a Snapshot of RAMP on VMware](#).

Note

The remaining upgrade steps are service-impacting.

6. Delete the RAMP instance:
 - a. Enter the VMware host machine IP address in a web browser and log on with your VMware credentials.
 - b. Shut down the RAMP virtual machine instance.
 - c. In the **Navigator** pane under **Virtual Machines**, right-click the RAMP instance and select **Delete**.
 - d. Confirm the deletion when prompted.
7. Instantiate an instance of RAMP using the latest version of the software. Refer to [Installing RAMP on VMware Manually](#).

Note

For an upgrade scenario, skip the "Install RAMP licenses" step.

8. (Optional) If you manage the SBC Edge devices with the RAMP, run the following:


```
/opt/sonus/ems/conf/edge_view_config add
```

 For more information, refer to [Deploy Optional Services on RAMP](#).
9. Restore the backed-up data on RAMP. For more information, refer to [Restore from Backup on RAMP Standalone](#).
10. Perform post-upgrade procedures. For more information, refer to [Post-Upgrade Procedures for RAMP](#).

Take a Snapshot of RAMP on VMware

You can take a snapshot of a [Ribbon Application Management Platform \(RAMP\)](#) standalone instance on VMware to store information on its current state. If an upgrade fails or needs to be reverted, a snapshot simplifies restoring the previous version of RAMP.

To take a snapshot of a RAMP VM:

Start

1. Enter the VMware host machine IP address in a web browser.
2. In the **Navigator** pane under **Virtual Machines**, select the RAMP virtual machine instance.
3. Click **Actions** at the top of the window and select **Snapshots > Take snapshot** from the drop-down menu.
The **Take snapshot for <name of the VM>** window opens, where you can define parameters for the snapshot.
4. Enter a name for the snapshot.
5. Enter a description for the snapshot.

6. Click **Take snapshot** to store the snapshot.
7. In the **Navigator** pane under **Storage**, click on **datastore**.
8. In the **Datastore browser**, check that the name of the snapshot you created appears to confirm that the snapshot is saved.

Upgrade RAMP GR on VMware

Related articles:

- [Tear Down RAMP GR](#)
- [Installing RAMP on VMware Manually](#)
- [Configuring RAMP GR](#)

Use the following procedure to upgrade a geographically redundant (GR) pair of Ribbon Application Management Platform (RAMP) instances on VMware. A RAMP GR deployment consists of an active and standby pair of instances. During this procedure, you will back up your current database and copy it to new instances with the current version of the RAMP software installed.

Prerequisites

- A host is available to store the backup.
- Ribbon recommends stopping RAMP before taking a backup.

Start

1. Copy the `insight` and `admin` user SSH keys to a secure, external location:
 - To obtain the SSH keys for the `insight` user, complete the procedure on [Obtain the RAMP SSH Keys](#).
 - To obtain the SSH keys for the `admin` user, repeat the same procedure except for the `admin` keys, SSH to the RAMP IP address as the `admin` user (instead of the `insight` user):

```
ssh admin@10.14.55.120
```

2. Log on to the VMware host.

Note

The remaining upgrade steps are service-impacting. Do not configure anything during the upgrade, as data may be lost.

3. Tear down the RAMP GR configuration to separate the instances. Refer to [Tear Down RAMP GR](#).
4. Upgrade the configured active RAMP instance. Refer to [Upgrade RAMP Standalone on VMware](#).
5. Perform the following to delete the standby RAMP instance and create a new RAMP instance using the latest version.
 - a. (Optional) Take a snapshot of the standby RAMP Virtual Machine (VM) to check if you need to revert it to the prior version of the standby RAMP. For more information, refer to [Take a Snapshot of RAMP on VMware](#).
 - b. Delete the standby RAMP instance:
 - i. Enter the VMware host machine IP address in a web browser and log on with your VMware credentials.
 - ii. Shut down the standby RAMP VM instance.

- iii. In the **Navigator** pane under **Virtual Machines**, right-click the standby RAMP instance and select **Delete**.
- iv. Confirm the deletion when prompted.
- c. Instantiate an instance of the standby RAMP using the latest software version. For more information, refer to [Installing RAMP on VMware Manually](#).
- d. (Optional) If you manage SBC Edge devices using RAMP and backed up, then deploy the optional services on RAMP. For more information, refer to [Deploy Optional Services on RAMP](#).
6. (Optional) In the case of an auto switchover enabled RAMP, you can upgrade the ETCD VMs to the latest available or released version. For more information, refer to [Upgrading etcd](#). Refer to the software bundles section of the latest release notes [RAMP Release Information](#).
7. Complete GR configuration for the pair of **RAMP** instances, using the configured active as the active instance. Refer to [Configuring RAMP GR](#).
8. Perform post-upgrade procedures on the active RAMP instance. Refer to [Post-Upgrade Procedures for RAMP](#).

Revert RAMP Upgrade on VMware

If you [took a snapshot](#) of your Ribbon Application Management Platform (RAMP) VM prior to an upgrade, you can use the snapshot to revert to your prior version of RAMP, if necessary.

To restore the RAMP VM from a snapshot:

1. Enter the VMware host machine IP address in a web browser.
2. In the **Navigator** pane under **Virtual Machines**, select the **RAMP** virtual machine instance.
3. Perform one of the following depending on whether you want to revert using the most recent snapshot or an earlier snapshot:
 - Revert to the most recent snapshot:
 - i. At the top of the window, click **Actions**, and then select **Snapshots > Restore snapshot** from the drop-down menu.
The **Restore latest snapshot** confirmation window opens.
 - ii. Click **Restore**.
 - Revert to an earlier snapshot.
 - i. At the top of the window, click **Actions**, and then select **Snapshots > Manage snapshot** from the drop-down menu.
The **Manage snapshots** window opens.
 - ii. Select the snapshot you want to use to restore your system.
 - iii. Click **Restore snapshot**.
The **Restore snapshot** confirmation window opens.
 - iv. Click **Restore**.
The RAMP restore process starts.
4. Follow the messages under **Recent tasks**. When the messages indicate that reset of the VM has completed successfully, check the **RAMP** status to verify that **RAMP** is at the desired version and that RAMP processes are running. Refer to [Check RAMP Status](#).

Upgrading RAMP in Public Cloud Environments

In this section:

- [Upgrading RAMP on AWS](#)
- [Upgrading RAMP on Azure](#)

Upgrading RAMP on AWS

You can manually upgrade the Ribbon Application Management Platform (RAMP) in an Amazon Web Services (AWS) environment using the procedures outlined in this topic.

Prerequisites

- Ribbon recommends viewing the warning notices about this release to see if your software or virtual resource requirements are affected.
- If you have an account on the Ribbon Support Portal, the warning notices are available at <https://ribboncommunications.com/services/ribbon-support-portal-login>.
- If you do not have a Ribbon Support Portal login account, contact the Ribbon Global Product Support (GPS).
- A host is available to store the backup.
- Ribbon recommends stopping RAMP before taking a backup.

The following workflow provides an overview of the process, including links to the specific information and steps required to complete the deployment. After completing the steps on the linked page, return to the workflow for the next procedure.

Step	Action
1	Take a look at the pre-upgrade checklist. For more information, refer to, Pre-Upgrade Checklist .
2	Take backup from the RAMP node (source for GR) and copy it to a remote server. For more information, refer to, Take a Backup of RAMP for Daily Maintenance .
3	Note Ensure that termination protection is disabled for the RAMP instance. Refer to https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/terminating-instances.html#Using_ChangingDisableAPITermination. Note For an upgrade, you must attach the instance to an external EBS volume. If the external EBS volume is not present in the instance, you cannot proceed with the upgrade.

Step	Action
4	Note down the following Stack Parameters of the RAMP instance. • To know the existing secondary volume id, navigate to EC2 > Instances > Select your instances > Storage > Under block devices. • Instance name. • New AMID. • Reuse the IP address of the existing RAMP instance on the upgraded RAMP. Based on the type of instance, reuse the following IP addresses: ◦ RAMP with a private IP address. Note the private management IP address of RAMP and reuse it. ◦ RAMP with a public IP address. Note both, the public and private management IP addresses of RAMP and reuse it.
5	Delete the RAMP stack. 1. Log on to the AWS. 2. Click Services and the AWS Services list displays. 3. Click CloudFormation from Management Tools section. 4. Select the stacks. 5. Click Delete. Note • Once the stack is deleted, the external EBS volume remains intact. You must use the volume ID of this external volume to create a new instance. • Store the private IP of the instance for later use.
6	Instantiate a RAMP instance with the following: • Instantiate a Standalone RAMP Instance on AWS with Public IP Address • Instantiate a Standalone RAMP Instance on AWS with Private IP Address
7	Rediscover the RAMP nodes. For example, rediscover localhost. For more information, refer to, How to Rediscover the localhost.
9	Perform post-upgrade procedures. For more information, refer to, Post-Upgrade Procedures for RAMP. Note • If any of the SBC or PSX nodes fail during the upgrade, you can instantiate new nodes using the same IP address. • The new SBC/PSX nodes are registered on the EMS node with the same IP address. • The new node will come up with the same configuration by reusing the IP address in the same cluster.

Upgrading RAMP on Azure

You can manually upgrade Ribbon Application Management Platform (RAMP) in an Azure using the procedures outlined in this topic.

Prerequisites

- Ribbon recommends that you view the warning notices pertaining to this release to see if your software or virtual resource requirements are affected.
- If you have an account on Ribbon Support Portal, you can find the warning notices at <https://ribboncommunications.com/services/ribbon-support-portal-login>.
- If you do not have a Ribbon Support Portal login account, you can contact the Ribbon Global Product Support (GPS).
- A host is available to store the backup.
- Ribbon recommends stopping RAMP before taking a backup.

The following workflow provides an overview of the process including links to the specific information and steps required to complete the deployment. After completing the steps on the linked page, return to the workflow for the next procedure.

Step	Action
1	Take a look at the pre-upgrade checklist. For more information, refer to, Pre-Upgrade Checklist .
2	Take backup from the RAMP node (source for GR) and copy it to a remote server. For more information, refer to, Take a Backup of RAMP for Daily Maintenance .
3	Note For an upgrade, you must attach the instance to an external EBS volume. If the external EBS volume is not present in the instance, you cannot proceed with the upgrade. Note down Stack Parameters of the RAMP instance. - For public template: - The hostname of RAMP. - The network interface name. - The data disk name and resource ID. - private (id_rsa) and public (id_rsa.pub) ssh keys of admin and insight from <code>/home/admin/.ssh</code> and <code>/opt/sonus/ems/.ssh</code> respectively - For private template: - The hostname of RAMP. - The private IP address. - The network interface name. - The data disk name and resource ID. - private (id_rsa) and public (id_rsa.pub) ssh keys of admin and ems from <code>/home/admin/.ssh</code> and <code>/opt/sonus/ems/.ssh</code> respectively.

Step	Action
4	Delete the Virtual Machine (VM) of RAMP instance: 1. Log onto the Microsoft Azure portal. 2. Navigate to Virtual Machines. 3. Select the VM to be deleted. 4. The VM page displays. 5. Click Delete. 6. From the list which asks you what all you wish to delete, delete only the VM and the OS disk. Retain the data disk, network interface and the public IP (if there is a public IP).
5	Instantiate a RAMP instance. Refer to the following • Generate Output Payload from createUIDefinition Sandbox • Instantiate a Standalone RAMP Instance on Azure.
6	Replace the private (id_rsa) and public (id_rsa.pub) ssh keys of admin and insight at: 1. <code>/home/admin/.ssh</code> (admin ssh key location) 2. <code>/opt/sonus/ems/.ssh</code> (insight ssh key location) with the older ssh key files that were manually saved earlier in step 3.
7	Rediscover the RAMP nodes. For example, rediscover localhost. For more information, refer to, How to Rediscover the localhost.
8	Install new licenses for the RAMP nodes. For more information, refer to, License Management.
9	Perform post-upgrade procedures. For more information, refer to, Post-Upgrade Procedures for RAMP.
10	Reboot the SBC and PSX nodes on EMS. Note • If any of the SBC or PSX nodes fail during the upgrade, you can instantiate new nodes using the same IP address. • The new SBC/PSX nodes are registered on the EMS node with the same IP address. • The new node will come up with the same configuration by reusing the IP address in the same cluster.

Upgrading RAMP CNF

Related articles:

- [RAMP CNF - Pre-Upgrade Checklist](#)
- [RAMP CNF - Upgrade RAMP GR Instance Using Helm Commands](#)
- [RAMP CNF - Upgrade RAMP GR Instance Using GIT](#)
- [RAMP CNF - Post-Upgrade Procedures](#)
- [Establish RAMP CNF Active-Standby Instance Passwordless Connection](#)

This section provides procedures to upgrade the installed Ribbon Application Management Platform (RAMP) Cloud Native Functionality (CNF) using Helm charts and GitOps.

Prerequisites

- Ensure you are aware of the passwords for all default RAMP accounts.
- Note the licenses available on your system. This helps in verifying the list of licenses after an upgrade. For more information, refer to [License Management](#).
- Check the database and file replication status on the GR deployment to ensure that synchronization is current. For more information, refer to [Check Database and File Replication Status](#).
- Take a back up of the RAMP active instance and copy it to a remote system. For more information, refer to [Take a Backup of RAMP for Daily Maintenance](#).
- Export performance management data from the RAMP active instance to an external server. For more information, refer to [Collect and Export Device Statistics](#).
- Copy RAMP's SSH keys , `authorized_keys` , and `known_hosts` for the insight user on both the active and standby instances to a remote server. For more information, refer to [Obtain the RAMP SSH Keys](#).

Procedure

Based on the current type of installation, select an upgrade procedure:

Upgrade Method	Procedure
Upgrade RAMP CNF using Helm charts	• RAMP CNF - Upgrade Standalone Instance Using Helm Commands • RAMP CNF - Upgrade RAMP GR Instance Using Helm Commands
Upgrade RAMP CNF using Git	• RAMP CNF - Upgrade Standalone Instance Using GIT • RAMP CNF - Upgrade RAMP GR Instance Using GIT

RAMP CNF - Pre-Upgrade Checklist

Accomplish these tasks at least seven days prior to starting the Ribbon Application Management Platform (RAMP) upgrade:

	Task
1	Check terminal and user access 1. Check that terminal/jumpserver access to RAMP is available. 2. Check that Insight, Postgres, and root passwords are available.
2	Verify release interoperability with other Ribbon products in your network Ensure that other elements integrated with RAMP are aligned with the target RAMP release according to the Ribbon Application Management Platform Interoperability Matrix.
3	Review Release Notes Review the release notes for RAMP configuration requirements before you upgrade. Some examples are software configuration requirements and upgrade notes under 'Install and upgrade notes' sections.
4	Prepare software 1. Review the RN 'Software Bundle' section to identify the application software files required for the upgrade. 2. Follow the upgrade section applicable to your RAMP environment for the location of where to transfer the application files. 3. Follow Download Files from Ribbon Support Portal for instructions to obtain software and create target directories for application files on the RAMP.
5	Check RAMP status 1. Confirm all processes are running. For more information, refer to Check RAMP Status. 2. For RAMP GR, check the replication status prior to the upgrade. For more information, refer to Check Database and File Replication Status. 3. Check whether API, CLI, PM, FM, PSX Manager, SBC Manager, and other core RAMP functions are operational.
6	Review upgrade prerequisites Review documentation section 'Upgrade prerequisites' or 'Prerequisites' based on the RAMP environment.

	Task
7	Check Hostname 1. Check whether the RAMP hostname matches installation requirements. 2. Hostname value using hostname command must match values on <code>/etc/hosts</code> and <code>/etc/sysconfig/network</code> configuration files. 3. The hostname configuration is case sensitive. 4. For Hostname/Instance name conventions, For more information, refer to Hostname and Instance Name Conventions.
8	Check managed elements Verify communication between RAMP and the managed elements. Find the nodes for which the RAMP discovery failed. 1. Open the file <code>/opt/devMgmt/logs/reachability_audit_log</code>. 2. Search for the string "timeout". Example: <pre>2023-06-19 18:31:16,875 IST INFO [Reachability_Worker-38] NotificationManager - localhost, SNMP, 10.54.141.91, 161, 5, RESPONSE timeout, <reachability count>, <node name>, <IP address of the node></pre> 3. Rediscover the non-cloud nodes for which RAMP discovery failed.

RAMP CNF - Upgrade Standalone Instance Using Helm Commands

Related articles:

- [Upgrading RAMP CNF](#)
- [Take a Backup of RAMP for Daily Maintenance](#)
- [Post-Upgrade Procedures for RAMP](#)

Use the following procedure to upgrade a standalone instance of the Ribbon Application Management Platform (RAMP) on a RAMP Cloud Native Function (CNF). During this procedure, you will back up your current database and copy it to the new instance with the current version of RAMP software installed.

Prerequisites

The prerequisites are listed on the [Upgrading RAMP CNF](#) page.

Start

1. Take a backup of the RAMP; refer to [Take a Backup of RAMP for Daily Maintenance](#).
2. Upgrade the active RAMP CNF using the `helm` command:

```
helm upgrade <deployment name> --values values.yaml .
```

Example:

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$ helm ls
sanramp          ems-svt-2      1      2023-05-24 22:57:24.532918309 +053
0 IST deployed   rbbn-ramp-cnf-23.06.00-50      1.0
```

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$ oc get pod -o wide
NAME                READY  STATUS   RESTARTS  AGE    IP             NODE
NOMINATED NODE    READINESS GATES
sanramp-rampcnf-0    2/2    Running   0          18m    10.231.13.134  worker-6.blr-ocp1.lab.rbbn.com
worker-6.blr-ocp1.lab.rbbn.com  <none>    <none>
```

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$
```

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$ helm upgrade sanramp -f values_blr1.yaml .
I0524 23:22:44.872839 1295865 request.go:665] Waited for 1.018790332s due to
client-side throttling, not priority and fairness, request: GET:https://api.blr-
ocp1.lab.rbbn.com:6443/apis/integreatly.org/v1alpha1?timeout=32s
Release "sanramp" has been upgraded. Happy Helming!
NAME: sanramp
LAST DEPLOYED: Wed May 24 23:22:51 2023
NAMESPACE: ems-svt-2
STATUS: deployed
REVISION: 2
TEST SUITE: None
NOTES:
```

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$
```

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$ oc get pod -o wide
sanramp-rampcnf-0    0/2    ContainerCreating   0          24s    <none>
worker-6.blr-ocp1.lab.rbbn.com  <none>    <none>
```

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$
```

```
[ssequeira@cli-blr-1 ~]$ oc get pod -o wide
NAME                READY  STATUS   RESTARTS  AGE    IP             NODE
NOMINATED NODE    READINESS GATES
sanramp-rampcnf-0    2/2    Running   0          7h58m    10.231.13.137  worker-6.blr-ocp1.lab.rbbn.com
worker-6.blr-ocp1.lab.rbbn.com  <none>    <none>
```

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$
```

```
[ssequeira@cli-blr-1 ~]$ oc get pvc | grep sanramp-rampcnf-0
sanramp-pmstats-pvc-sanramp-rampcnf-0          Bound      pvc-43efbbee-afcd-456b-
a994-0d258d9ae4cc      20Gi       RWX          managed-nfs-storage      8h
sanramp-ramp-pv-storage-sanramp-rampcnf-0      Bound      pvc-f80916d7-095a-4fbf-
bf44-8eef0ee24ad4      150Gi      RWO          csi-rbd-sc               8h
sanramp-rbbn-otel-agent-pvc-sanramp-rampcnf-0  Bound      pvc-06bdaaba-52c4-4775-
8cdb-c7ac52d2ce26      20Gi       RWX          managed-nfs-storage      8h
[ssequeira@cli-blr-1 ~]$
```

```
[ssequeira@cli-blr-1 ~]$ helm history sanramp
REVISION          UPDATED              STATUS          CHART
APP VERSION      DESCRIPTION
1                 Wed May 24 22:57:24 2023    superseded     rbbn-ramp-cnf-23.0
6.00-50          1.0                 Install complete
2                 Wed May 24 23:22:51 2023    deployed      rbbn-ramp-cnf-23.0
6.00-55          1.0                 Upgrade complete
[ssequeira@cli-blr-1 ~]$
```

3. Check the status of the active RAMP CNF. For more information, refer to [Check RAMP Status](#).

Note

Before you proceed, ensure the active RAMP CNF is running.

4. Perform post-upgrade procedures on the active RAMP CNF. For more information, refer to [Post-Upgrade Procedures for RAMP](#).

RAMP CNF - Upgrade RAMP GR Instance Using Helm Commands

In this section:

- [RAMP CNF Upgrade using Helm Commands](#)
- [Post-Upgrade Procedure](#)

Related articles:

- [Upgrading RAMP CNF](#)
- [Tear Down RAMP GR](#)
- [Check RAMP Status](#)
- [Post-Upgrade Procedures for RAMP](#)
- [How to Start and Stop RAMP](#)
- [Copy SSH Keys to Instantiate a RAMP Standby Instance](#)
- [How to Rediscover the localhost](#)
- [Establish RAMP CNF Active-Standby Instance Passwordless Connection](#)

Use the following procedure to upgrade a Geographically Redundant (GR) pair of Ribbon Application Management Platform (RAMP) pods. A RAMP GR deployment consists of a pair of active and standby pods. During this procedure, copy the backup of your current database to the new instances along with the current version of RAMP

Use this procedure to upgrade the RAMP CNF using Helm commands.

Prerequisites

The prerequisites listed in the [Upgrading RAMP CNF](#) page.

RAMP CNF Upgrade using Helm Commands

Start

1. Tear down the GR configuration. For more information, refer to [Tear Down RAMP GR](#). After you tear down the GR configuration, database changes are no longer in sync (including servicing the network) between the RAMP active and standby RAMP CNF. The teardown process stops database replication and makes the RAMP active and standby CNFs work as standalone CNFs.
2. Check the status of the **RAMP** standby CNF. For more information, refer to [Check RAMP Status](#).

Before you proceed, ensure the standby CNF is running.

3. Upgrade the active RAMP CNF using Helm command:

```
cd <root directory of the Helm chart>
helm upgrade <release_name> .
```

Example:

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$ helm ls
sanramp          ems-svt-2      1      2023-05-24 22:57:24.532918309 +053
0 IST deployed   rbbn-ramp-cnf-23.06.00-50      1.0
```

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$ oc get pod -o wide
NAME              READY  STATUS   RESTARTS  AGE    IP             NODE
NOMINATED NODE   READINESS GATES
sanramp-rampcnf-0 2/2    Running  0         18m    10.231.13.134  worker-6.blr-ocp1.lab.rbbn.com
worker-6.blr-ocp1.lab.rbbn.com  <none>    <none>
```

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$ helm upgrade sanramp -f values_blr1.yaml .
I0524 23:22:44.872839 1295865 request.go:665] Waited for 1.018790332s due to
client-side throttling, not priority and fairness, request: GET:https://api.blr-
ocp1.lab.rbbn.com:6443/apis/integreatly.org/v1alpha1?timeout=32s
Release "sanramp" has been upgraded. Happy Helming!
NAME: sanramp
LAST DEPLOYED: Wed May 24 23:22:51 2023
NAMESPACE: ems-svt-2
STATUS: deployed
REVISION: 2
```

TEST SUITE: None
NOTES:

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$
```

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$ oc get pod -o wide
sanramp-rampcnf-0      0/2      ContainerCreating    0          24s      <none>
worker-6.blr-ocp1.lab.rbbn.com  <none>    <none>
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$
```

```
[ssequeira@cli-blr-1 ~]$ oc get pod -o wide
NAME                  READY   STATUS    RESTARTS   AGE   IP             NODE
NOMINATED NODE      READINESS GATES
sanramp-rampcnf-0      2/2     Running   0           7h58m  10.231.13.137  worker-6.blr-ocp1.lab.rbbn.com
worker-6.blr-ocp1.lab.rbbn.com  <none>    <none>
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$
```

```
[ssequeira@cli-blr-1 ~]$ oc get pvc | grep sanramp-rampcnf-0
sanramp-pmstats-pvc-sanramp-rampcnf-0      Bound      pvc-43efbbee-afcd-456b-a994-0d258d9ae4cc    20Gi      RWX      managed-nfs-storage    8h
sanramp-ramp-pv-storage-sanramp-rampcnf-0  Bound      pvc-f80916d7-095a-4fbf-bf44-8eef0ee24ad4    150Gi     RWO      csi-rbd-sc             8h
sanramp-rbbn-otel-agent-pvc-sanramp-rampcnf-0  Bound      pvc-06bdaaba-52c4-4775-8cdb-c7ac52d2ce26    20Gi      RWX      managed-nfs-storage    8h
[ssequeira@cli-blr-1 ~]$
```

```
[ssequeira@cli-blr-1 ~]$ helm history sanramp
REVISION      UPDATED              STATUS      CHART
APP VERSION   DESCRIPTION
1             Wed May 24 22:57:24 2023    superseded  rbbn-ramp-cnf-23.0
6.00-50       1.0                 Install complete
2             Wed May 24 23:22:51 2023    deployed   rbbn-ramp-cnf-23.0
6.00-55       1.0                 Upgrade complete
[ssequeira@cli-blr-1 ~]$
```

4. Check the status of the active RAMP CNF. For more information, refer to [Check RAMP Status](#).

Note

Before you proceed, ensure the active RAMP CNF is running.

5. Check if the `SSH keys`, `authorized_keys`, and `known_hosts` for the insight user on the active RAMP CNF are the same as the entries you recorded before the upgrade.

Note

When restoring the database, these files are replaced with the files available in the PVC.

6. Perform post-upgrade procedures on the active RAMP CNF. For more information, refer to [Post-Upgrade Procedures for RAMP](#).
7. Stop the standby RAMP CNF. For more information, refer to [How to Start and Stop RAMP](#).

At this point, the active RAMP CNF contains the database.

8. Upgrade the standby RAMP pod:

```
helm upgrade <release_name> .
```

9. Copy the SSH key of the new active RAMP CNF to the standby RAMP CNF. For more information, refer to [Copy SSH Keys to Instantiate a RAMP Standby Instance](#).
10. Check the status of the standby RAMP CNF. For more information, refer to [Check RAMP Status](#).

Before you proceed further, ensure that the standby RAMP CNF is running.

11. Ensure the `SSH keys`, `authorized_keys`, and `known_hosts` for the insight user in the standby RAMP CNF are the same as before the upgrade.
12. On the active RAMP CNF, configure GR parameters. For more information, refer to [Configuring RAMP GR](#).

There may be Performance Management (PM) collection data loss for around 15 minutes while configuring GR.

Additionally, the PM data collected by the standby RAMP CNF while recreating the active RAMP CNF is lost while configuring **RAMP GR**. During upgrade, the data sync does not occur between the **RAMP standby** and **active RAMP CNF**.

13. The status of the active and standby RAMP CNFs may show as offline on the upgraded RAMP. Rediscover both active and standby RAMP CNFs. For more information, refer to [How to Rediscover the localhost](#).
14. Ensure password-less SSH connection is working from the RAMP active to standby RAMP CNF and vice versa. For more information, refer to [Establish RAMP CNF Active-Standby Instance Passwordless Connection](#).

Post-Upgrade Procedure

After you perform an upgrade, you must perform post-upgrade procedures. For more information, refer to [RAMP CNF - Post-Upgrade Procedures](#).

RAMP CNF - Upgrade Standalone Instance Using GIT

Related articles:

- [Upgrading RAMP CNF](#)
- [Take a Backup of RAMP for Daily Maintenance](#)
- [Post-Upgrade Procedures for RAMP](#)

Use the following procedure to upgrade a Standalone instance of the Ribbon Application Management Platform (RAMP) on an instance of the Cloud Native Function (CNF). During this procedure, copy the backup of your current database to the new instances along with the current version of RAMP.

Prerequisites

The prerequisites listed in the [Upgrading RAMP CNF](#) page.

Start

1. Take a backup of the RAMP. For more information, refer to [Take a Backup of RAMP for Daily Maintenance](#).
2. Check the status of the RAMP standby instance. For more information, refer to [Check RAMP Status](#).
3. Perform the following steps to create RAMP CNF:
 - a. Create the RAMP CNF deployment `.yaml` file based on the requirements:

Example:

```
# Values for RBBN-CORE-CNF chart
# This is a YAML-formatted file.
# Declare variables to be passed into your templates.

apiVersion: helm.toolkit.fluxcd.io/v2beta1
kind: HelmRelease
metadata:
  name: sanjay-blr-ramp
  namespace: ramp-svt
spec:
  releaseName: sanjay-blr-ramp
  targetNamespace: ramp-svt
  chart:
    spec:
      chart: rbbn-ramp-cnf
      version: 23.06.00-81
      sourceRef:
        kind: HelmRepository
        name: ramp-helm-prod-plano
        namespace: ramp-svt
  install:
    disableWait: true
  upgrade:
    disableWait: true
```

```

interval: 5m
timeout: 10m
values:
  global:

    # Namespace this helm chart will be deployed
    # This is optional. You could set to "" to use default namespace
    namespace: "ramp-svt"

    # Override obs storageClassName
    # This is optional. You could set to "" to use default storageClassName
    storageClassName: "managed-nfs-storage"

    ns_uuid: "8aebafe4-50c2-4f52-a43f-b7d1a40df51c"
    cnf_uuid: "e56aa2ea-2c1e-4964-970e-b86eaff727d9"
    cnfc_uuid: "b3e021dc-947d-4c19-824b-3412c267509f"

    certManager:
      enabled: true
      issuer:
        name: "cross-cluster-ca-selfsigned-clusterissuer"
        ## @param global.certManager.issuer.kind The Issuer kind to sign
the certificate request. Can be "Issuer" or "ClusterIssuer"
        kind: "ClusterIssuer"

    auth:
      kafkaClient:
        secureTransport: true
        certFilename: cert.pem
        certKeyFilename: key.pem
        caFilename: "ca.pem"

        ## @param auth.client.certDuration Requested duration the signed
certificate will be valid for
        certDuration: ""

        ## @param auth.client.certExtraDnsSans DNS Subject Alternative Name
to add to the certificates
        certExtraDnsSans: ""

        ## @param auth.client.certExtraIpSans IP Subject Alternative Name
to add to the certificates
        certExtraIpSans: ""

        ## @param auth.client.existingSecret Name of the existing secret
containing the TLS certificates for client-to-server communications
        existingSecret: ""

    # Base RBBN_OBS container image.
    # RCO: artifactory-tx.rbbn.com
    # BLR: artifact2.eng.sonusnet.com
    imageRegistry: artifact2.eng.sonusnet.com

```

```

# If you need kubernetes secret to pull from private repo. You will
need username and access token
# For example:
# To get the access token:
# curl -u <windowsUsername>:<'<windowsPasswd>' -X POST https://
artifact2.eng.sonusnet.com/artifactory/api/security/token -d
"username=<windowsUsername>" -d "expires_in=86400" -d "refreshable=true" -d
"scope=member-of-groups:readers" -d "audience=jfirt@*"
# Replace windowUsername and windowPassword with appropriate username
and password.
# set imageCredentials: {} if you don't secret to pull from private
repo
imageCredentials:
  create: false
  #Private repo for ribbon images
  registry: artifact2.eng.sonusnet.com
  username: ssequeira
  password:
eyJ2ZXIiOiIyIiwidHlwIjoisldUIiwYXNjoiUlMyNTYiLCJraWQiOiJ0b2Z0emxGZGtnSjdaW
FZnRnRTTm94RzBLMTE3ZEZldEVaVXd5YVg3a2xVIn0.eyJzdWIiOiJqZnJ0QDAXY2RyYnJwejljYz
c1MXFnemI5bTIxaHB1XC91c2Vyc1wvc3NlcXVlaXJhIiwic2NwIjoibWVtYmVyLW9mLWdyb3Vwc3p
yZWFKZXJzIiwiaXVkaIjoiamZydEAqIiwiaXNzIjoiamZydEAWMWNkcWJycHo5Y2M3NTFfZ3piOW0y
MWhwZVwvdXNlc3NzZXFlZWlyYSIsImV4cCI6MTcxMTM2NjYzMiwiawF0IjoxNjc5ODMwNjMyL
CJqdGkiOiI3ODYwZjczMC1mODRkLTQyNjgtYmQ4NC03MTc5MmUwZDFLZWEifQ.G_MdtWQsQqHExz0
X9L5wGvkk8HYnEfs87f0b1-5tcICeJ73B_aHIUYwFQRsa40ykmtUDTmkDKTzT0kaQ8NCVstbLuFvi
RRgSxsafjPG4wdqnHZyF6Pq-NJZIsuKHGhtG59tHg1erq8nlyEAE-
_GHdVhivQtbsMfhAuFUJlG2xI8obeUWS8MWjQv2u301HPHcJv7QlIF8aX01p7EuqwmMidGnSM_wik
wMT4cl4nAbq0xh00y7glPVkE5TquKFH909vhzyWpvpSds0BCrMLTjR6Cy1wmvz5u5YiSS2rEG0q96
j2KveSEYstJyVe1Ug0L_gnc4pv6Iie7Poc--pta4_Qg

# Override obs image for aggregator and agent
# This is required if you enable rbbn_obs (See below rbbn_obs.enabled =
true)
obs:
  image:
    repository: ribbon-telemetry-docker-prod-plano/release/
rbbn-telemetry_collector
    tag: v1.3.5
    pullPolicy: Always

# Log rotation mechanism for the Observability server
obsLogRetentionPolicy:
# represent the percentage of the disk usage on when log rotation
will be trigger.
# I.e. A 20Gb storage limit request for a PVC with a
rotateTriggerPercent set at 50 (50%)
# means that log rotation will be trigger when disk will reach 10Gb
rotateTriggerPercent: 50
# Choice are "minute" "hourly" "daily" "weekly"
# recurringInterval represent the period of time on when we want to
check if disk usage has surpass the threshold.
recurringInterval: "hourly"

```

```

    role:
      # Specifies whether a Role and RoleBinding should be created for
the observability components
      create: true

    serviceAccount:
      # Specifies whether a service account should be created for the
observability components
      create: false
      # Annotations to add to the service account
      annotations: {}
      # The name of the service account to use.
      # If not set and create is true, a name is generated using the
fullname template
      name: default

    # Storage request limit for PVC
    logPersistentVolumeStorage:
      use: false
      request: 20Gi
      annotations:
        volume.beta.kubernetes.io/storage-provisioner: storage.io/nfs

    logs:
      # Name of secret that contains Elasticsearch credentials
      elasticsearchSecretName: ""
      # Name of secret that contains Elasticsearch credentials, evaluated
as a template, for example "{{.Release.Name }}-elasticsearch-user-cred"
      elasticsearchSecretNameTemplate: ""
      # Name of secret that contains Kafka credentials
      kafkaSecretName: ""
      # Name of secret that contains Kafka credentials, evaluated as a
template, for example "{{.Release.Name }}-kafka-user-cred"
      kafkaSecretNameTemplate: ""

      # Backend server configuration can be read here as an alternative
to the obs.logs section
      backendServers:

    #Timezone for ramp pod
    # This is optional. Comment it out if not needed. It will default to
UTC if not provided.
    timeZone: "Asia/Kolkata"

    # Platform on which the Ribbon RAMP CNe solution is deployed.
    # Allowed values - ocp, robin
    kubernetesPlatform: ocp

    # robin platform wants to be able to specify static_ip_policy in
annotations
    # accepted values are ippool,range

```

```

static_ip_policy: "ippool"

# Template strings to evaluate to existing secret to use to pull
images, for example: name: "{{.Release.Name }}-imagecred"
imagePullSecretTemplates:
  - name: "{{.Release.Name }}-imagecred"

# Values for rbbn-ramp chart
rbbn-ramp:
  #Ramp image
  # This is required
  rampImage:
    repository: ems-docker-prod-plano/production/rampcnf/rbbn-ramp-cnf
    pullPolicy: IfNotPresent
    # This is the ramp version
    tag: "23.06.00-81"
    #tag: "22.05.00-131"

# Define addition external interfaces for ramp pod
# This is required. Ramp requires eth1 for management access and eth2
for LI.
networkInterface:
  # Either 'ipv4' or 'ipv6'
  ipversion: "ipv4"
  #Number of external interface for ramp
  numberOfExternalInterface: 1
  # This is the interface for management access - devices, GR, etc.
  eth1:
    interface: ext-static-net-3
    ip: "10.52.80.129"
    prefix: "24"
    gateway: "10.52.80.1"
    routes:
      - destIp: 10.70.0.0
        prefix: "16"
      - destIp: 10.54.0.0
        prefix: "16"
      - destIp: 10.52.0.0
        prefix: "16"
      - destIp: 10.32.0.0
        prefix: "16"
      - destIp: 10.34.0.0
        prefix: "16"
      - destIp: 10.33.0.0
        prefix: "16"
      - destIp: 172.21.0.0
        prefix: "16"
      - destIp: 172.19.0.0
        prefix: "16"
      - destIp: 172.29.0.0
        prefix: "16"
  # This is the interface for LI

```



```

eth2:
  interface: ext-static-net-4
  ip: ""
  prefix: ""
  gateway: ""
  routes:
    - destIp: ""
      prefix: ""

# Ramp kubernetes service
# "port" exposes the Kubernetes service on the specified port within
the cluster. Other pods within the cluster can communicate with this server
on the specified port
# "type" could be "ClusterIP", "NodePort" and "LoadBalancer". Refer to
kubernetes service for more detail.
# Set enabled: false if not needed.
rampService:
  enabled: false
  port: 443
  type: ClusterIP

auth:
  # etcd client TLS certificate
  etcdclient:
    certManager:
      # enabled: switch to enable cert-manager to generate and manage
the etcd client certificate
      # NOTE: Set this to true only if global.certManager.enabled is
set to true and network.interfaceName
      # is set to eth1 and the network attachment used for eth1 is
configured to assign static IPs.
      enabled: true
      ## @param auth.client.certExtraDnsSans DNS Subject Alternative
Name to add to the certificates
      ##
      certExtraDnsSans: ""
      ## @param auth.client.certExtraIpSans IP Subject Alternative Name
to add to the certificates
      ##
      certExtraIpSans: ""
      # certDuration: duration in hours, minutes, or seconds that the
certificate should be valid for
      # NOTE: If certDuration is not specified (""), then the
certificate will be valid
      # for 90 days by default and will be renewed 30 days before
expiry. The minimum value for
      # certDuration is 1 hour.
      # Example:
      # If the duration needs to be 180 days, then this can be
specified as below:
      #   certDuration: 4320h
      certDuration: ""

```

```

alarm:
  exporters:
    - enabled: false
      type: kafka
      config:
        bootstrap_servers:
          - ip: 127.0.0.1
            port: 9092
        topic: ""
        format: json
        standard: ETSI_S0L003
        properties: # producer configuration can be provided here with
proper indentation
#       security.protocol: SSL
#       ssl.kafka.private.key.location: /opt/fm/kafka/certs/key.pem
#       ssl.kafka.public.cert.location: /opt/fm/kafka/certs/cert.pem
#       ssl.kafka.ca.cert.location: /opt/fm/kafka/certs/ca.pem

# The memory/cpu limits will be equals to requests to esure pod gets
assigned a QoS class of Guaranteed
# Required
rampResources:
  requests:
    cpu: 16
    memory: 64Gi
#   hugepages:
  limits:
#   hugepages: 2Gi

# Persistent for ramp container
rampPersistent:
  #Storage class class for ramp. User could configure diffirent
storageClassName for obs(global section)
  #storageClass is optional field.
  #storageClassName is optional. Comment it out if you want to use
default storageClassName.
  storageClassName: "csi-rbd-sc"

# storageAccessMode for ramp
#ReadWriteOnce - the volume can be mounted as read-write by a single
node
#ReadOnlyMany - the volume can be mounted read-only by many nodes
#ReadWriteMany - the volume can be mounted as read-write by many
nodes
# storageAccessMode is required field
storageAccessMode: "ReadWriteOnce"

# Storage size. Required field.
storage: "130Gi"

# Enable or disable startupProbe, livenessProbe, and readinessProbe

```

```

probe: True

#Assigning Pods to Nodes with specific label
#For example:
nodeSelector: {}
#nodeSelector:
# kubernetes.io/hostname: worker-9.blr-ocp1.lab.rbbn.com

# Set this for kubernetes tolerations
# Optional
tolerations: []

# Set this for kubernetes affinity
# Optional
affinity: {}

# Set the namespaces for antiaffinity rule
anti_affinity_namespaces: ["ramp-svt", "sbc-svt-regr", "psx-svt","ems-
dev", "ems-svt-perf", "ems-svt","ats-dev","ems-svt-2","platform-dev","platfor
m-svt","psx-dev","raf-dev","rampev-svt","sbx-dev","sbc-svt","psx-cnf-svt",
"cnf-demolab", "sbc-dev-tekton", "ramp-svt", "ems-svt-perf", "cats-svt"]

#Use this to inject public keys for users. Set it to
# Optional
#Users: [] if not needed.
users:
- name: "admin"
  # To generate password for "admin" user, run "openssl passwd -6
admin"
  password:
"$6$lQMeZQPJoaXfchXn$2jYBgDqj9ubRTRMgPwoDQg87358IBY7pV9FmBf/
VNN57htbOWP9DezDgXp30mo7LthuHbDjFekrAWxB8UQ/tt1"
  ssh_authorized_keys:
- ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIE1q9aASBnezCE+irhepjrzSuY4w0hkNBUyQ0uqnCgeT
admin@rbbn.com
- name: "insight"
  # To generate password for "insight" user, run "openssl passwd -6
insight"
  password: "$6$WDZgaeEQY007xZLg$SVZ/OQL/.VUF/dFu/
1M.rxfNq0JdxSXNHciPqKwduuyoS0y6iLnN2kZ/qbLhMVVDwarQYmbCB22C9pGZ.BT8f1"
  ssh_authorized_keys:
- ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIE1q9aASBnezCE+irhepjrzSuY4w0hkNBUyQ0uqnCgeT
insight@rbbn.com

# You only need to modify this if you want to use rbbn-sdrp
# Set enabled: true if you want to enable sdrp for ramp. Default to
false
rbbn_sdrp:
  enabled: false
  fqdn_instance: ""

```

```

# You only need to modify this if you want to use rbbn-obs
# Set enabled: true if you want to enable observability agent for ramp.
Default to true
rbbn_obs:
  enabled: true

# Service for obs sidecar within pod.
obsService:
  type: ClusterIP
  port: 9101
  ipFamilyPolicy: SingleStack # Allowed values PreferDualStack or
SingleStack.According the below value should be altered
  ipFamilies:
    - IPv4

resources:
  rbbn_telemetry_agent:
    limits:
      cpu: 4
      memory: 8Gi
    #requests:
    #  cpu: 100m
    #  memory: 128Mi

# Add the pod annotations to enable prometheus discovery and
scraping.
# port we are exposing for prometheus scraping.
# This port should match the service port and the server metric
output endpoint.
podAnnotations:
  prometheus.io/path: "/metrics"
  prometheus.io/scrape: true
  prometheus.io/port: "9101"
  prometheus.io/scheme: "http"

serviceLabels:
  component: prometheus-rbbn-otel-agent
  tenant: ramp
  servicetype: observability

configMap:
  metrics:
    enable: True
  appStats:
    scrapeInterval: 5s
    endpoints:
      - addr: "localhost:10050"
        containerName: rbbn-rampcnf-container
    output:
      - server: "prometheus"

```

```

        endpoint: "0.0.0.0:9101"
    logs:
        enable: True
        defaultTopic: default # log messages to this Kafka topic by
default when a topic for the container parsers or system is not specified
        system: True
        systemTopic: system # system logs will be sent to this Kafka
topic, defaultTopic is used if this property is not defined
        telemetry:
            enable: True # Process the otel agent logs
            topic: rbbn-otel-agent # Open telemetry logs will be sent to
this Kafka topic
        podlogs: True
        logPrefix:
            nodeId: True
            containerId: True
        kafkaSecretName: ""
        backendServers: # Example of backend servers
            stdout:
                enable: False
            elasticsearch: []
            # - endpoint: elasticsearch.apps.rco-ocp1.lab.rbbn.com:443
            #   auth: True
            #   username: ELASTICSEARCH_USER
            #   password: ELASTICSEARCH_PASSWD
            #   index: platform-filebeat
            kafka: []
            # - endpoint: elasticsearch.apps.rco-ocp1.lab.rbbn.com:12345
            #   sslCert: KAFKA_CERT
            #   sslKey: KAFKA_KEY
            #   sslCa: KAFKA_CA
    # elasticsearch Credentials
    elasticsearchCreds:
        create: False
        #user:
        #key: ELASTICSEARCH_USER
        #value:
        #password:
        #key: ELASTICSEARCH_PASSWD
        #value:
    # KAFKA Credentials
    # all values should be base64 encoded.
    kafkaCreds:
        create: False
        path: /etc/kafka/ssl
        sslCert:
            key: KAFKA_CERT
            value:
        sslKey:
            key: KAFKA_KEY
            value:
        sslCa:

```

```

        key: KAFKA_CA
        value:

## sdrp subchart values
sdrp-operator:
  common-util:
    logPersistentVolumeStorage:
      create: false
    imageCredentials:
      # Specifies whether an image credentials secret should be created as a
      post-delete hook
      createPostDelete: true

## @section sdrp-operator container parameters
operator:

  ## @param sdrp-operator image parameters
  image:
    ## @param operator.image.repository sdrp-operator image name
    repository: ccs-docker-prod-virtual/sdrp-operator

  ## @section sdr container parameters
  ##
  ## @param sdr.clusterScopeRegistry.enabled Create a backend
  configuration for the cluster scope if equal true
  ## @param sdr.globalScopeRegistry Specify the initial backend
  configuration for the global scope to use in the sdr container
  ## @param nameservers - [array] List of DNS nameserver. Syntax:
  ip:port. If port if not specified, port 53 is used
  ## @param domain - Name of the domain to publish to in the service
  registry for the cluster scope
  ## @param tsigKeyName - Name of the TSIG key attached to DNS messages
  ## @param tsigSecret - TSIG (base64) value attached to DNS messages
  ## @param tsigSecretAlg - TSIG algorithm. Supported value: hmac-md5,
  hmac-sha1, hmac-sha256, hmac-sha512
  ##
  sdr:
    ## @param sdrp-operator image parameters
    image:
      ## @param operator.image.repository sdrp-operator image name
      repository: service_discovery-docker-prod-ottawa/sdr

  clusterScopeRegistry:
    enabled: true
    nameservers: []
    domain: ""
    tsigKeyName: ""
    tsigSecret: ""
    tsigSecretAlg: ""
  globalScopeRegistry:
    enabled: true
    nameservers: []

```

```
domain: ""
tsigKeyName: ""
tsigSecret: ""
tsigSecretAlg: ""
```

- b. Create the `kustomization.yaml` file to include the RAMP CNF deployment file name.

```
apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization
nameSuffix: -ssequira
resources:
  - values_ramp.yaml    ---> This is the name of the HelmRelease file.
```

- c. Commit and Push the changes using git commands.

```
[ssequira@cli-blr-2 jenkinsbuild-dev]$ git add -A; git commit -a -m "upgrading
active ramp"; git push origin master
[master 88562d8] installing ramp
 1 file changed, 1 insertion(+), 1 deletion(-)
Counting objects: 11, done.
Delta compression using up to 24 threads.
Compressing objects: 100% (5/5), done.
Writing objects: 100% (6/6), 530 bytes | 0 bytes/s, done.
Total 6 (delta 3), reused 0 (delta 0)
To ssh://git@bitbucket.rbbn.com:7999/ems/rbbn-cnf-gitops-ramp-svt.git
 01f6ef4..88562d8 master -> master
[ssequira@cli-blr-2 jenkinsbuild-dev]$
```

4. Check the status of the RAMP CNF. For more information, refer to [Check RAMP Status](#).
5. Perform post-upgrade procedures on the RAMP CNF. For more information, refer to [RAMP CNF - Post-Upgrade Procedures](#).

RAMP CNF - Upgrade RAMP GR Instance Using GIT

In this section:

- [RAMP CNF Upgrade Using Git](#)
- [Post-Upgrade Procedure](#)

Related articles:

- [Upgrading RAMP CNF](#)
- [RAMP CNF - Pre-Upgrade Checklist](#)
- [Tear Down RAMP GR](#)
- [Check RAMP Status](#)
- [RAMP CNF - Post-Upgrade Procedures](#)
- [How to Start and Stop RAMP](#)
- [Copy SSH Keys to Instantiate a RAMP Standby Instance](#)
- [How to Rediscover the localhost](#)
- [Establish RAMP CNF Active-Standby Instance Passwordless Connection](#)

Use the following procedure to upgrade a Geographically Redundant (GR) pair of Ribbon Application Management Platform (RAMP) on Cloud Native Function (CNF) instances. A RAMP GR deployment consists of an Active and Standby instance pair. During this procedure, copy the backup of your current database to the new instances along with the current version of RAMP.

Use this procedure to upgrade RAMP CNF using Git commands.

Prerequisites

The prerequisites listed in the [Upgrading RAMP CNF](#) page.

RAMP CNF Upgrade Using Git

Use this procedure to upgrade RAMP CNF using Git.

Start

1. Tear down the GR configuration. For more information, refer to [Tear Down RAMP GR](#).
After you tear down the GR configuration, database changes are no longer in sync (including servicing the network) between the RAMP Active and Standby instances. The teardown process stops database replication and makes the RAMP Active and Standby instances work as standalone instances.
2. Check the status of the RAMP Standby instance. For more information, refer to [Check RAMP Status](#).

Before you proceed, ensure the Standby instance is running.

3. Create an Active instance:
 - a. Create the RAMP CNF deployment `.yaml` file based on the requirements:

```
# Values for RBBN-CORE-CNF chart
# This is a YAML-formatted file.
# Declare variables to be passed into your templates.

apiVersion: helm.toolkit.fluxcd.io/v2beta1
kind: HelmRelease
metadata:
  name: sanjay-blr-ramp
  namespace: ramp-svt
spec:
  releaseName: sanjay-blr-ramp
  targetNamespace: ramp-svt
  chart:
    spec:
      chart: rbbn-ramp-cnf
      version: 23.06.00-81
      sourceRef:
        kind: HelmRepository
        name: ramp-helm-prod-plano
        namespace: ramp-svt
  install:
    disableWait: true
  upgrade:
    disableWait: true
```



```

interval: 5m
timeout: 10m
values:
  global:

    # Namespace this helm chart will be deployed
    # This is optional. You could set to "" to use default namespace
    namespace: "ramp-svt"

    # Override obs storageClassName
    # This is optional. You could set to "" to use default storageClassName
    storageClassName: "managed-nfs-storage"

    ns_uuid: "8aebafe4-50c2-4f52-a43f-b7d1a40df51c"
    cnf_uuid: "e56aa2ea-2c1e-4964-970e-b86eaff727d9"
    cnfc_uuid: "b3e021dc-947d-4c19-824b-3412c267509f"

    certManager:
      enabled: true
      issuer:
        name: "cross-cluster-ca-selfsigned-clusterissuer"
        ## @param global.certManager.issuer.kind The Issuer kind to sign
the certificate request. Can be "Issuer" or "ClusterIssuer"
        kind: "ClusterIssuer"

    auth:
      kafkaClient:
        secureTransport: true
        certFilename: cert.pem
        certKeyFilename: key.pem
        caFilename: "ca.pem"

        ## @param auth.client.certDuration Requested duration the signed
certificate will be valid for
        certDuration: ""

        ## @param auth.client.certExtraDnsSans DNS Subject Alternative Name
to add to the certificates
        certExtraDnsSans: ""

        ## @param auth.client.certExtraIpSans IP Subject Alternative Name
to add to the certificates
        certExtraIpSans: ""

        ## @param auth.client.existingSecret Name of the existing secret
containing the TLS certificates for client-to-server communications
        existingSecret: ""

    # Base RBBN_OBS container image.
    # RCO: artifactory-tx.rbbn.com
    # BLR: artifact2.eng.sonusnet.com
    imageRegistry: artifact2.eng.sonusnet.com

```

```

# If you need kubernetes secret to pull from private repo. You will
need username and access token
# For example:
# To get the access token:
# curl -u <windowsUsername>:<'<windowsPasswd>' -X POST https://
artifact2.eng.sonusnet.com/artifactory/api/security/token -d
"username=<windowsUsername>" -d "expires_in=86400" -d "refreshable=true" -d
"scope=member-of-groups:readers" -d "audience=jfirt@*"
# Replace windowUsername and windowPassword with appropriate username
and password.
# set imageCredentials: {} if you don't secret to pull from private
repo
imageCredentials:
  create: false
  #Private repo for ribbon images
  registry: artifact2.eng.sonusnet.com
  username: ssequeira
  password:
eyJ2ZXIiOiIyIiwidHlwIjoisldUIiwYXNjoiUlMyNTYiLCJraWQiOiJ0b2Z0emxGZGtnSjdaW
FZnRnRTTm94RzBLMTE3ZEZldEVaVXd5YVg3a2xVIn0.eyJzdWIiOiJqZnJ0QDAXY2RyYnJwejljYz
c1MXFnemI5bTIxaHB1XC91c2Vyc1wvc3NlcXVlaXJhIiwic2NwIjoibWVtYmVyLW9mLWdyb3Vwc3p
yZWFKZXJzIiwiaXVkaWoiZmZyZjczMC1mODRkLTQyNjgtYmQ4NC03MTc5MmUwZDFLZWEifQ.G_MdtWQsQqHExz0
X9L5wGvkk8HYnEfs87f0b1-5tcICeJ73B_aHIUYwFQRsa40ykmtUDTmkDKTzT0kaQ8NCVstbLuFvi
RRgSxsafjPG4wdqnHZyF6Pq-NJZIsuKHGhtG59tHg1erq8nlyEAE-
_GHdVhivQtbsMfhAuFUJlG2xI8obeUWS8MWjQv2u301HPHcJv7QlIF8aX01p7EuqwmMidGnSM_wik
wMT4cl4nAbq0xh00y7glPVkE5TquKFH909vhzyWpvpSds0BCrMLTjR6Cy1wmvz5u5YiSS2rEG0q96
j2KveSEYstJyVe1Ug0L_gnc4pv6Iie7Poc--pta4_Qg

# Override obs image for aggregator and agent
# This is required if you enable rbbn_obs (See below rbbn_obs.enabled =
true)
obs:
  image:
    repository: ribbon-telemetry-docker-prod-plano/release/
rbbn_telemetry_collector
    tag: v1.3.5
    pullPolicy: Always

# Log rotation meachanise for the Observability server
obsLogRetentionPolicy:
# represent the percentage of the disk usage on when log rotation
will be trigger.
# I.e. A 20Gb storage limit request for a PVC with a
rotateTriggerPercent set at 50 (50%)
# means that log rotation will be trigger when disk will reach 10Gb
rotateTriggerPercent: 50
# Choice are "minute" "hourly" "daily" "weekly"
# recurringInterval represent the period of time on when we want to
check if disk usage has surpass the threshold.
recurringInterval: "hourly"

```

```

    role:
      # Specifies whether a Role and RoleBinding should be created for
the observability components
      create: true

    serviceAccount:
      # Specifies whether a service account should be created for the
observability components
      create: false
      # Annotations to add to the service account
      annotations: {}
      # The name of the service account to use.
      # If not set and create is true, a name is generated using the
fullname template
      name: default

    # Storage request limit for PVC
    logPersistentVolumeStorage:
      use: false
      request: 20Gi
      annotations:
        volume.beta.kubernetes.io/storage-provisioner: storage.io/nfs

    logs:
      # Name of secret that contains Elasticsearch credentials
      elasticsearchSecretName: ""
      # Name of secret that contains Elasticsearch credentials, evaluated
as a template, for example "{{.Release.Name }}-elasticsearch-user-cred"
      elasticsearchSecretNameTemplate: ""
      # Name of secret that contains Kafka credentials
      kafkaSecretName: ""
      # Name of secret that contains Kafka credentials, evaluated as a
template, for example "{{.Release.Name }}-kafka-user-cred"
      kafkaSecretNameTemplate: ""

      # Backend server configuration can be read here as an alternative
to the obs.logs section
      backendServers:

    #Timezone for ramp pod
    # This is optional. Comment it out if not needed. It will default to
UTC if not provided.
    timeZone: "Asia/Kolkata"

    # Platform on which the Ribbon RAMP CNe solution is deployed.
    # Allowed values - ocp, robin
    kubernetesPlatform: ocp

    # robin platform wants to be able to specify static_ip_policy in
annotations
    # accepted values are ippool,range

```

```

static_ip_policy: "ippool"

# Template strings to evaluate to existing secret to use to pull
images, for example: name: "{{.Release.Name }}-imagecred"
imagePullSecretTemplates:
  - name: "{{.Release.Name }}-imagecred"

# Values for rbbn-ramp chart
rbbn-ramp:
  #Ramp image
  # This is required
  rampImage:
    repository: ems-docker-prod-plano/production/rampcnf/rbbn-ramp-cnf
    pullPolicy: IfNotPresent
    # This is the ramp version
    tag: "23.06.00-81"
    #tag: "22.05.00-131"

# Define addition external interfaces for ramp pod
# This is required. Ramp requires eth1 for management access and eth2
for LI.
networkInterface:
  # Either 'ipv4' or 'ipv6'
  ipversion: "ipv4"
  #Number of external interface for ramp
  numberOfExternalInterface: 1
  # This is the interface for management access - devices, GR, etc.
  eth1:
    interface: ext-static-net-3
    ip: "10.52.80.129"
    prefix: "24"
    gateway: "10.52.80.1"
    routes:
      - destIp: 10.70.0.0
        prefix: "16"
      - destIp: 10.54.0.0
        prefix: "16"
      - destIp: 10.52.0.0
        prefix: "16"
      - destIp: 10.32.0.0
        prefix: "16"
      - destIp: 10.34.0.0
        prefix: "16"
      - destIp: 10.33.0.0
        prefix: "16"
      - destIp: 172.21.0.0
        prefix: "16"
      - destIp: 172.19.0.0
        prefix: "16"
      - destIp: 172.29.0.0
        prefix: "16"
  # This is the interface for LI

```

```

eth2:
  interface: ext-static-net-4
  ip: ""
  prefix: ""
  gateway: ""
  routes:
    - destIp: ""
      prefix: ""

# Ramp kubernetes service
# "port" exposes the Kubernetes service on the specified port within
the cluster. Other pods within the cluster can communicate with this server
on the specified port
# "type" could be "ClusterIP", "NodePort" and "LoadBalancer". Refer to
kubernetes service for more detail.
# Set enabled: false if not needed.
rampService:
  enabled: false
  port: 443
  type: ClusterIP

auth:
  # etcd client TLS certificate
  etcdclient:
    certManager:
      # enabled: switch to enable cert-manager to generate and manage
the etcd client certificate
      # NOTE: Set this to true only if global.certManager.enabled is
set to true and network.interfaceName
      # is set to eth1 and the network attachment used for eth1 is
configured to assign static IPs.
      enabled: true
      ## @param auth.client.certExtraDnsSans DNS Subject Alternative
Name to add to the certificates
      ##
      certExtraDnsSans: ""
      ## @param auth.client.certExtraIpSans IP Subject Alternative Name
to add to the certificates
      ##
      certExtraIpSans: ""
      # certDuration: duration in hours, minutes, or seconds that the
certificate should be valid for
      # NOTE: If certDuration is not specified (""), then the
certificate will be valid
      # for 90 days by default and will be renewed 30 days before
expiry. The minimum value for
      # certDuration is 1 hour.
      # Example:
      # If the duration needs to be 180 days, then this can be
specified as below:
      #   certDuration: 4320h
      certDuration: ""

```

```

alarm:
  exporters:
    - enabled: false
      type: kafka
      config:
        bootstrap_servers:
          - ip: 127.0.0.1
            port: 9092
        topic: ""
        format: json
        standard: ETSI_S0L003
        properties: # producer configuration can be provided here with
proper indentation
#       security.protocol: SSL
#       ssl.kafka.private.key.location: /opt/fm/kafka/certs/key.pem
#       ssl.kafka.public.cert.location: /opt/fm/kafka/certs/cert.pem
#       ssl.kafka.ca.cert.location: /opt/fm/kafka/certs/ca.pem

# The memory/cpu limits will be equals to requests to esure pod gets
assigned a QoS class of Guaranteed
# Required
rampResources:
  requests:
    cpu: 16
    memory: 64Gi
#   hugepages:
  limits:
#   hugepages: 2Gi

# Persistent for ramp container
rampPersistent:
  #Storage class class for ramp. User could configure diffirent
storageClassName for obs(global section)
  #storageClass is optional field.
  #storageClassName is optional. Comment it out if you want to use
default storageClassName.
  storageClassName: "csi-rbd-sc"

# storageAccessMode for ramp
#ReadWriteOnce - the volume can be mounted as read-write by a single
node
#ReadOnlyMany - the volume can be mounted read-only by many nodes
#ReadWriteMany - the volume can be mounted as read-write by many
nodes
# storageAccessMode is required field
storageAccessMode: "ReadWriteOnce"

# Storage size. Required field.
storage: "130Gi"

# Enable or disable startupProbe, livenessProbe, and readinessProbe

```

```

probe: True

#Assigning Pods to Nodes with specific label
#For example:
nodeSelector: {}
#nodeSelector:
# kubernetes.io/hostname: worker-9.blr-ocp1.lab.rbbn.com

# Set this for kubernetes tolerations
# Optional
tolerations: []

# Set this for kubernetes affinity
# Optional
affinity: {}

# Set the namespaces for antiaffinity rule
anti_affinity_namespaces: ["ramp-svt", "sbc-svt-regr", "psx-svt","ems-
dev", "ems-svt-perf", "ems-svt","ats-dev","ems-svt-2","platform-dev","platfor
m-svt","psx-dev","raf-dev","rampev-svt","sbx-dev","sbc-svt","psx-cnf-svt",
"cnf-demolab", "sbc-dev-tekton", "ramp-svt", "ems-svt-perf", "cats-svt"]

#Use this to inject public keys for users. Set it to
# Optional
#Users: [] if not needed.
users:
- name: "admin"
  # To generate password for "admin" user, run "openssl passwd -6
admin"
  password:
"$6$lQMeZQPJoaXfchXn$2jYBgDqj9ubRTRMgPwoDQg87358IBY7pV9FmBf/
VNN57htbOWP9DezDgXp30mo7LthuHbDjFekrAWxB8UQ/tt1"
  ssh_authorized_keys:
- ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIE1q9aASBnezCE+irhepjrzSuY4w0hkNBUyQ0uqnCgeT
admin@rbbn.com
- name: "insight"
  # To generate password for "insight" user, run "openssl passwd -6
insight"
  password: "$6$WDZgaeEQY007xZLg$SVZ/OQL/.VUF/dFu/
1M.rxfNq0JdxSXNHciPqKwduuyoS0y6iLnN2kZ/qbLhMVVDwarQYmbCB22C9pGZ.BT8f1"
  ssh_authorized_keys:
- ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIE1q9aASBnezCE+irhepjrzSuY4w0hkNBUyQ0uqnCgeT
insight@rbbn.com

# You only need to modify this if you want to use rbbn-sdrp
# Set enabled: true if you want to enable sdrp for ramp. Default to
false
rbbn_sdrp:
  enabled: false
  fqdn_instance: ""

```

```

# You only need to modify this if you want to use rbbn-obs
# Set enabled: true if you want to enable observability agent for ramp.
Default to true
rbbn_obs:
  enabled: true

# Service for obs sidecar within pod.
obsService:
  type: ClusterIP
  port: 9101
  ipFamilyPolicy: SingleStack # Allowed values PreferDualStack or
SingleStack.According the below value should be altered
  ipFamilies:
    - IPv4

resources:
  rbbn_telemetry_agent:
    limits:
      cpu: 4
      memory: 8Gi
    #requests:
    #  cpu: 100m
    #  memory: 128Mi

# Add the pod annotations to enable prometheus discovery and
scraping.
# port we are exposing for prometheus scraping.
# This port should match the service port and the server metric
output endpoint.
podAnnotations:
  prometheus.io/path: "/metrics"
  prometheus.io/scrape: true
  prometheus.io/port: "9101"
  prometheus.io/scheme: "http"

serviceLabels:
  component: prometheus-rbbn-otel-agent
  tenant: ramp
  servicetype: observability

configMap:
  metrics:
    enable: True
  appStats:
    scrapeInterval: 5s
    endpoints:
      - addr: "localhost:10050"
        containerName: rbbn-rampcnf-container
    output:
      - server: "prometheus"

```



```

        endpoint: "0.0.0.0:9101"
    logs:
        enable: True
        defaultTopic: default # log messages to this Kafka topic by
default when a topic for the container parsers or system is not specified
        system: True
        systemTopic: system # system logs will be sent to this Kafka
topic, defaultTopic is used if this property is not defined
        telemetry:
            enable: True # Process the otel agent logs
            topic: rbbn-otel-agent # Open telemetry logs will be sent to
this Kafka topic
        podlogs: True
        logPrefix:
            nodeId: True
            containerId: True
        kafkaSecretName: ""
        backendServers: # Example of backend servers
            stdout:
                enable: False
            elasticsearch: []
            # - endpoint: elasticsearch.apps.rco-ocp1.lab.rbbn.com:443
            #   auth: True
            #   username: ELASTICSEARCH_USER
            #   password: ELASTICSEARCH_PASSWD
            #   index: platform-filebeat
            kafka: []
            # - endpoint: elasticsearch.apps.rco-ocp1.lab.rbbn.com:12345
            #   sslCert: KAFKA_CERT
            #   sslKey: KAFKA_KEY
            #   sslCa: KAFKA_CA
# elasticsearch Credentials
elasticsearchCreds:
    create: False
    #user:
        #key: ELASTICSEARCH_USER
        #value:
    #password:
        #key: ELASTICSEARCH_PASSWD
        #value:
# KAFKA Credentials
# all values should be base64 encoded.
kafkaCreds:
    create: False
    path: /etc/kafka/ssl
    sslCert:
        key: KAFKA_CERT
        value:
    sslKey:
        key: KAFKA_KEY
        value:
    sslCa:

```

```

        key: KAFKA_CA
        value:

## sdrp subchart values
sdrp-operator:
  common-util:
    logPersistentVolumeStorage:
      create: false
    imageCredentials:
      # Specifies whether an image credentials secret should be created as a
      post-delete hook
      createPostDelete: true

## @section sdrp-operator container parameters
operator:

  ## @param sdrp-operator image parameters
  image:
    ## @param operator.image.repository sdrp-operator image name
    repository: ccs-docker-prod-virtual/sdrp-operator

  ## @section sdr container parameters
  ##
  ## @param sdr.clusterScopeRegistry.enabled Create a backend
  configuration for the cluster scope if equal true
  ## @param sdr.globalScopeRegistry Specify the initial backend
  configuration for the global scope to use in the sdr container
  ## @param nameservers - [array] List of DNS nameserver. Syntax:
  ip:port. If port if not specified, port 53 is used
  ## @param domain - Name of the domain to publish to in the service
  registry for the cluster scope
  ## @param tsigKeyName - Name of the TSIG key attached to DNS messages
  ## @param tsigSecret - TSIG (base64) value attached to DNS messages
  ## @param tsigSecretAlg - TSIG algorithm. Supported value: hmac-md5,
  hmac-sha1, hmac-sha256, hmac-sha512
  ##
  sdr:
    ## @param sdrp-operator image parameters
    image:
      ## @param operator.image.repository sdrp-operator image name
      repository: service_discovery-docker-prod-ottawa/sdr

  clusterScopeRegistry:
    enabled: true
    nameservers: []
    domain: ""
    tsigKeyName: ""
    tsigSecret: ""
    tsigSecretAlg: ""
  globalScopeRegistry:
    enabled: true
    nameservers: []

```

```
domain: ""
tsigKeyName: ""
tsigSecret: ""
tsigSecretAlg: ""
```

- b. Create the `kustomization.yaml` file to include the RAMP CNF deployment file name.

```
apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization
nameSuffix: -ssequira
resources:
  - values_ramp.yaml ---> This is the name of the HelmRelease file.
```

- c. Commit and Push the changes:

```
[ssequira@cli-blr-2 jenkinsbuild-dev]$ git add -A; git commit -a -m "upgrading
active ramp"; git push origin master
[master 88562d8] installing ramp
 1 file changed, 1 insertion(+), 1 deletion(-)
Counting objects: 11, done.
Delta compression using up to 24 threads.
Compressing objects: 100% (5/5), done.
Writing objects: 100% (6/6), 530 bytes | 0 bytes/s, done.
Total 6 (delta 3), reused 0 (delta 0)
To ssh://git@bitbucket.rbbn.com:7999/ems/rbbn-cnf-gitops-ramp-svt.git
 01f6ef4..88562d8 master -> master
[ssequira@cli-blr-2 jenkinsbuild-dev]$
```

4. Check the status of the RAMP Active instance. For more information, refer to [Check RAMP Status](#).

Before you proceed, ensure the Active instance is running.

5. Check if the SSH keys, `authorized_keys`, and `known_hosts` for the insight user on the RAMP Active instance are the same as the entries you recorded before the upgrade.

When restoring the database, these files are replaced with the files available in the Cinder volume.

6. Perform post-upgrade procedures on the RAMP Active instance. For more information, refer to [RAMP CNF - Post-Upgrade Procedures](#).
7. Stop the RAMP Standby instance. For more information, refer to [How to Start and Stop RAMP](#).

At this point, the RAMP Active instance contains the database.

8. To create a Standby instance:

- a. Copy the SSH key of the new RAMP Active instance to the Standby instance. For more information, refer to [Copy SSH Keys to Instantiate a RAMP Standby Instance](#).
- b. Create the RAMP CNF deployment `.yaml` file based on the requirements:

Example

```
# Values for RBBN-CORE-CNF chart
# This is a YAML-formatted file.
# Declare variables to be passed into your templates.

apiVersion: helm.toolkit.fluxcd.io/v2beta1
kind: HelmRelease
metadata:
  name: sanjay-blr-ramp
  namespace: ramp-svt
spec:
  releaseName: sanjay-blr-ramp
  targetNamespace: ramp-svt
  chart:
    spec:
      chart: rbbn-ramp-cnf
      version: 23.06.00-81
      sourceRef:
        kind: HelmRepository
        name: ramp-helm-prod-plano
        namespace: ramp-svt
  install:
    disableWait: true
  upgrade:
    disableWait: true
  interval: 5m
  timeout: 10m
  values:
    global:

      # Namespace this helm chart will be deployed
      # This is optional. You could set to "" to use default namespace
      namespace: "ramp-svt"

      # Override obs storageClassName
      # This is optional. You could set to "" to use default storageClassName
      storageClassName: "managed-nfs-storage"

      ns_uuid: "8aebafe4-50c2-4f52-a43f-b7d1a40df51c"
      cnf_uuid: "e56aa2ea-2c1e-4964-970e-b86eaff727d9"
      cnfc_uuid: "b3e021dc-947d-4c19-824b-3412c267509f"

      certManager:
        enabled: true
        issuer:
```

```

    name: "cross-cluster-ca-selfsigned-clusterissuer"
    ## @param global.certManager.issuer.kind The Issuer kind to sign
the certificate request. Can be "Issuer" or "ClusterIssuer"
    kind: "ClusterIssuer"

auth:
  kafkaClient:
    secureTransport: true
    certFilename: cert.pem
    certKeyFilename: key.pem
    caFilename: "ca.pem"

    ## @param auth.client.certDuration Requested duration the signed
certificate will be valid for
    certDuration: ""

    ## @param auth.client.certExtraDnsSans DNS Subject Alternative Name
to add to the certificates
    certExtraDnsSans: ""

    ## @param auth.client.certExtraIpSans IP Subject Alternative Name
to add to the certificates
    certExtraIpSans: ""

    ## @param auth.client.existingSecret Name of the existing secret
containing the TLS certificates for client-to-server communications
    existingSecret: ""

    # Base RBBN_OBS container image.
    # RCO: artifactory-tx.rbbn.com
    # BLR: artifact2.eng.sonusnet.com
    imageRegistry: artifact2.eng.sonusnet.com

    # If you need kubernetes secret to pull from private repo. You will
need username and access token
    # For example:
    # To get the access token:
    # curl -u <windowsUsername>:<'<windowsPasswd>' -X POST https://
artifact2.eng.sonusnet.com/artifactory/api/security/token -d
"username=<windowsUsername>" -d "expires_in=86400" -d "refreshable=true" -d
"scope=member-of-groups:readers" -d "audience=jfrt@*"
    # Replace windowUsername and windowPassword with appropriate username
and password.
    # set imageCredentials: {} if you don't secret to pull from private
repo
    imageCredentials:
      create: false
      #Private repo for ribbon images
      registry: artifact2.eng.sonusnet.com
      username: ssequeira
      password:
eyJ2ZXIiOiIyIiwidHlwIjoisldUIiwYXNjoiUlMyNTYiLCJraWQiOiJ0b2Z0emxGZGtnSjdaW
FZnRnRTTm94RzBLMTE3ZEZldEVaVXd5YVg3a2xVIn0.eyJzdWIiOiJqZnJ0QDAXY2RyYnJwejljYz
c1MXFnemI5bTIxaHB1XC91c2Vyc1wvc3NlcXVlaXJhIiwic2NwIjoibWVtYmVyLW9mLWdyb3Vwczp

```

```
yZWfKZXJzIiwiYXVkiJoiamZydEAqIiwiaXNzIjoiamZydEAWMNkcWJycHo5Y2M3NTFxZ3piOW0y
MWhwZVwvdXNlcnNcL3NzZXFlZWlyYSIsImV4cCI6MTcxMTM2NjYzMiwiaWF0IjoxNjc5ODMwNjMyL
CJqdGkiOiI3ODYwZjczMC1mODRkLTQyNjgtYmQ4NC03MTc5MmUwZDFlZWVhZG90LWVhZG90LWVhZG90
X9L5wGvkk8HYnEfs87f0b1-5tcICeJ73B_aHIUYwFQRsa40ykmtUDTmkDKTzT0kaQ8NCVstbLuFvi
RRgSxsafjPG4wdqnHZyF6Pq-NJZIsuKHGhtG59tHg1erq8nlyEAE-
_GHdVhivQtbsMfhAuFUJlG2xI8obeUWS8MWjQv2u301HPHcJv7QlIF8aX01p7EuqwmMidGnSM_wik
wMT4cl4nAbq0xh00y7glPVkE5TquKFH909vhzyWpvpSds0BCrMLTjR6Cy1wmvz5u5YiSS2rEG0q96
j2KveSEYstJyVe1Ug0L_gnc4pv6Iie7Poc--pta4_Qg
```

```
# Override obs image for aggregator and agent
# This is required if you enable rbbn_obs (See below rbbn_obs.enabled =
true)
obs:
  image:
    repository: ribbon-telemetry-docker-prod-plano/release/
rbbn-telemetry_collector
    tag: v1.3.5
    pullPolicy: Always

# Log rotation mechanism for the Observability server
obsLogRetentionPolicy:
# represent the percentage of the disk usage on when log rotation
will be trigger.
# I.e. A 20Gb storage limit request for a PVC with a
rotateTriggerPercent set at 50 (50%)
# means that log rotation will be trigger when disk will reach 10Gb
rotateTriggerPercent: 50
# Choice are "minute" "hourly" "daily" "weekly"
# recurringInterval represent the period of time on when we want to
check if disk usage has surpass the threshold.
recurringInterval: "hourly"

role:
# Specifies whether a Role and RoleBinding should be created for
the observability components
create: true

serviceAccount:
# Specifies whether a service account should be created for the
observability components
create: false
# Annotations to add to the service account
annotations: {}
# The name of the service account to use.
# If not set and create is true, a name is generated using the
fullname template
name: default

# Storage request limit for PVC
logPersistentVolumeStorage:
  use: false
  request: 20Gi
```

```

        annotations:
            volume.beta.kubernetes.io/storage-provisioner: storage.io/nfs

    logs:
        # Name of secret that contains Elasticsearch credentials
        elasticsearchSecretName: ""
        # Name of secret that contains Elasticsearch credentials, evaluated
as a template, for example "{{.Release.Name }}-elasticsearch-user-cred"
        elasticsearchSecretNameTemplate: ""
        # Name of secret that contains Kafka credentials
        kafkaSecretName: ""
        # Name of secret that contains Kafka credentials, evaluated as a
template, for example "{{.Release.Name }}-kafka-user-cred"
        kafkaSecretNameTemplate: ""

        # Backend server configuration can be read here as an alternative
to the obs.logs section
        backendServers:

        #Timezone for ramp pod
        # This is optional. Comment it out if not needed. It will default to
UTC if not provided.
        timeZone: "Asia/Kolkata"

        # Platform on which the Ribbon RAMP CNe solution is deployed.
        # Allowed values - ocp, robin
        kubernetesPlatform: ocp

        # robin platform wants to be able to specify static_ip_policy in
annotations
        # accepted values are ippool,range
        static_ip_policy: "ippool"

        # Template strings to evaluate to existing secret to use to pull
images, for example: name: "{{.Release.Name }}-imagecred"
        imagePullSecretTemplates:
            - name: "{{.Release.Name }}-imagecred"

    # Values for rbbn-ramp chart
    rbbn-ramp:
        #Ramp image
        # This is required
        rampImage:
            repository: ems-docker-prod-plano/production/rampcnf/rbbn-ramp-cnf
            pullPolicy: IfNotPresent
            # This is the ramp version
            tag: "23.06.00-81"
            #tag: "22.05.00-131"

        # Define addition external interfaces for ramp pod
        # This is required. Ramp requires eth1 for management access and eth2
for LI.

```

```

networkInterface:
  # Either 'ipv4' or 'ipv6'
  ipversion: "ipv4"
  #Number of external interface for ramp
  numberOfExternalInterface: 1
  # This is the interface for management access - devices, GR, etc.
  eth1:
    interface: ext-static-net-3
    ip: "10.52.80.129"
    prefix: "24"
    gateway: "10.52.80.1"
    routes:
      - destIp: 10.70.0.0
        prefix: "16"
      - destIp: 10.54.0.0
        prefix: "16"
      - destIp: 10.52.0.0
        prefix: "16"
      - destIp: 10.32.0.0
        prefix: "16"
      - destIp: 10.34.0.0
        prefix: "16"
      - destIp: 10.33.0.0
        prefix: "16"
      - destIp: 172.21.0.0
        prefix: "16"
      - destIp: 172.19.0.0
        prefix: "16"
      - destIp: 172.29.0.0
        prefix: "16"
  # This is the interface for LI
  eth2:
    interface: ext-static-net-4
    ip: ""
    prefix: ""
    gateway: ""
    routes:
      - destIp: ""
        prefix: ""

  # Ramp kubernetes service
  # "port" exposes the Kubernetes service on the specified port within
  the cluster. Other pods within the cluster can communicate with this server
  on the specified port
  # "type" could be "ClusterIP", "NodePort" and "LoadBalancer". Refer to
  kubernetes service for more detail.
  # Set enabled: false if not needed.
  rampService:
    enabled: false
    port: 443
    type: ClusterIP

```



```

auth:
  # etcd client TLS certificate
  etcdclient:
    certManager:
      # enabled: switch to enable cert-manager to generate and manage
the etcd client certificate
      # NOTE: Set this to true only if global.certManager.enabled is
set to true and network.interfaceName
      # is set to eth1 and the network attachment used for eth1 is
configured to assign static IPs.
      enabled: true
      ## @param auth.client.certExtraDnsSans DNS Subject Alternative
Name to add to the certificates
      ##
      certExtraDnsSans: ""
      ## @param auth.client.certExtraIpSans IP Subject Alternative Name
to add to the certificates
      ##
      certExtraIpSans: ""
      # certDuration: duration in hours, minutes, or seconds that the
certificate should be valid for
      # NOTE: If certDuration is not specified (""), then the
certificate will be valid
      # for 90 days by default and will be renewed 30 days before
expiry. The minimum value for
      # certDuration is 1 hour.
      # Example:
      # If the duration needs to be 180 days, then this can be
specified as below:
      #   certDuration: 4320h
      certDuration: ""

alarm:
  exporters:
    - enabled: false
    type: kafka
    config:
      bootstrap_servers:
        - ip: 127.0.0.1
          port: 9092
      topic: ""
      format: json
      standard: ETSI_S0L003
      properties: # producer configuration can be provided here with
proper indentation
      #   security.protocol: SSL
      #   ssl.kafka.private.key.location: /opt/fm/kafka/certs/key.pem
      #   ssl.kafka.public.cert.location: /opt/fm/kafka/certs/cert.pem
      #   ssl.kafka.ca.cert.location: /opt/fm/kafka/certs/ca.pem

      # The memory/cpu limits will be equals to requests to esure pod gets
assigned a QoS class of Guaranteed

```

```

# Required
rampResources:
  requests:
    cpu: 16
    memory: 64Gi
#   hugepages:
  limits:
#   hugepages: 2Gi

# Persistent for ramp container
rampPersistent:
  #Storage class class for ramp. User could configure different
storageClassName for obs(global section)
  #storageClass is optional field.
  #storageClassName is optional. Comment it out if you want to use
default storageClassName.
  storageClassName: "csi-rbd-sc"

# storageAccessMode for ramp
#ReadWriteOnce - the volume can be mounted as read-write by a single
node
#ReadOnlyMany - the volume can be mounted read-only by many nodes
#ReadWriteMany - the volume can be mounted as read-write by many
nodes
# storageAccessMode is required field
storageAccessMode: "ReadWriteOnce"

# Storage size. Required field.
storage: "130Gi"

# Enable or disable startupProbe, livenessProbe, and readinessProbe
probe: True

#Assigning Pods to Nodes with specific label
#For example:
nodeSelector: {}
#nodeSelector:
# kubernetes.io/hostname: worker-9.blr-ocp1.lab.rbbn.com

# Set this for kubernetes tolerations
# Optional
tolerations: []

# Set this for kubernetes affinity
# Optional
affinity: {}

# Set the namespaces for antiaffinity rule
anti_affinity_namespaces: ["ramp-svt", "sbc-svt-regr", "psx-svt","ems-
dev", "ems-svt-perf", "ems-svt","ats-dev","ems-svt-2","platform-dev","platfor
m-svt","psx-dev","raf-dev","rampev-svt","sbx-dev","sbc-svt","psx-cnf-svt",
"cnf-demolab", "sbc-dev-tekton", "ramp-svt", "ems-svt-perf", "cats-svt"]

```

```

#Use this to inject public keys for users. Set it to
# Optional
#Users: [] if not needed.
users:
- name: "admin"
  # To generate password for "admin" user, run "openssl passwd -6
admin"
  password:
"$6$!QMeZQPJoaXfchXn$2jYBgDqj9ubRTRMgPwoDQg87358IBY7pV9FmBf/
VNN57htbOWP9DezDgXp30mo7LthuHbDjFekrAWxB8UQ/tt1"
  ssh_authorized_keys:
- ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIE1q9aASBnezCE+irhepjrzSuY4w0hkNBUyQ0uqnCgeT
admin@rbbn.com
- name: "insight"
  # To generate password for "insight" user, run "openssl passwd -6
insight"
  password: "$6$WDZgaeEQY007xZLg$SVZ/OQL/.VUF/dFu/
1M.rxfNq0JdxSXNHCIpQKwduuyoS0y6iLnN2kZ/qbLhMVVDwarQYmbCB22C9pGZ.BT8f1"
  ssh_authorized_keys:
- ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIE1q9aASBnezCE+irhepjrzSuY4w0hkNBUyQ0uqnCgeT
insight@rbbn.com

# You only need to modify this if you want to use rbbn-sdrp
# Set enabled: true if you want to enable sdrp for ramp. Default to
false
rbbn_sdrp:
  enabled: false
  fqdn_instance: ""

# You only need to modify this if you want to use rbbn-obs
# Set enabled: true if you want to enable observability agent for ramp.
Default to true
rbbn_obs:
  enabled: true

# Service for obs sidecar within pod.
obsService:
  type: ClusterIP
  port: 9101
  ipFamilyPolicy: SingleStack # Allowed values PreferDualStack or
SingleStack.According the below value should be altered
  ipFamilies:
- IPv4

resources:
  rbbn_telemetry_agent:
    limits:
      cpu: 4
      memory: 8Gi

```

```

#requests:
#  cpu: 100m
#  memory: 128Mi

# Add the pod annotations to enable prometheus discovery and
scraping.
# port we are exposing for prometheus scraping.
# This port should match the service port and the server metric
output endpoint.
podAnnotations:
  prometheus.io/path: "/metrics"
  prometheus.io/scrape: true
  prometheus.io/port: "9101"
  prometheus.io/scheme: "http"

serviceLabels:
  component: prometheus-rbbn-otel-agent
  tenant: ramp
  servicetype: observability

configMap:
  metrics:
    enable: True
    appStats:
      scrapeInterval: 5s
      endpoints:
        - addr: "localhost:10050"
          containerName: rbbn-rampcnf-container
    output:
      - server: "prometheus"
        endpoint: "0.0.0.0:9101"
  logs:
    enable: True
    defaultTopic: default # log messages to this Kafka topic by
default when a topic for the container parsers or system is not specified
    system: True
    systemTopic: system # system logs will be sent to this Kafka
topic, defaultTopic is used if this property is not defined
    telemetry:
      enable: True # Process the otel agent logs
      topic: rbbn-otel-agent # Open telemetry logs will be sent to
this Kafka topic
    podlogs: True
    logPrefix:
      nodeId: True
      containerId: True
    kafkaSecretName: ""
    backendServers: # Example of backend servers
      stdout:
        enable: False
      elasticsearch: []

```

```

        # - endpoint: elasticsearch.apps.rco-ocp1.lab.rbbn.com:443
        #   auth: True
        #   username: ELASTICSEARCH_USER
        #   password: ELASTICSEARCH_PASSWD
        #   index: platform-filebeat
kafka: []
        # - endpoint: elasticsearch.apps.rco-ocp1.lab.rbbn.com:12345
        #   sslCert: KAFKA_CERT
        #   sslKey: KAFKA_KEY
        #   sslCa: KAFKA_CA
# elasticsearch Credentials
elasticsearchCreds:
  create: False
  #user:
    #key: ELASTICSEARCH_USER
    #value:
  #password:
    #key: ELASTICSEARCH_PASSWD
    #value:
# KAFKA Credentials
# all values should be base64 encoded.
kafkaCreds:
  create: False
  path: /etc/kafka/ssl
  sslCert:
    key: KAFKA_CERT
    value:
  sslKey:
    key: KAFKA_KEY
    value:
  sslCa:
    key: KAFKA_CA
    value:

## sdrp subchart values
sdrp-operator:
  common-util:
    logPersistentVolumeStorage:
      create: false
  imageCredentials:
    # Specifies whether an image credentials secret should be created as a
    post-delete hook
    createPostDelete: true

## @section sdrp-operator container parameters
operator:

## @param sdrp-operator image parameters
image:
  ## @param operator.image.repository sdrp-operator image name
  repository: ccs-docker-prod-virtual/sdrp-operator

```

```

## @section sdr container parameters
##
## @param sdr.clusterScopeRegistry.enabled Create a backend
configuration for the cluster scope if equal true
## @param sdr.globalScopeRegistry Specify the initial backend
configuration for the global scope to use in the sdr container
## @param nameservers - [array] List of DNS nameserver. Syntax:
ip:port. If port if not specified, port 53 is used
## @param domain - Name of the domain to publish to in the service
registry for the cluster scope
## @param tsigKeyName - Name of the TSIG key attached to DNS messages
## @param tsigSecret - TSIG (base64) value attached to DNS messages
## @param tsigSecretAlg - TSIG algorithm. Supported value: hmac-md5,
hmac-sha1, hmac-sha256, hmac-sha512
##
sdr:
  ## @param sdrp-operator image parameters
  image:
    ## @param operator.image.repository sdrp-operator image name
    repository: service_discovery-docker-prod-ottawa/sdr

  clusterScopeRegistry:
    enabled: true
    nameservers: []
    domain: ""
    tsigKeyName: ""
    tsigSecret: ""
    tsigSecretAlg: ""
  globalScopeRegistry:
    enabled: true
    nameservers: []
    domain: ""
    tsigKeyName: ""
    tsigSecret: ""
    tsigSecretAlg: ""

```

- c. Create the `kustomization.yaml` file to include the RAMP CNF deployment file name.

```

apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization
nameSuffix: -ssequira
resources:
  - values_ramp.yaml    ---> This is the name of the HelmRelease file.

```

- d. Commit and Push the changes:

```

[ssequira@cli-blr-2 jenkinsbuild-dev]$ git add -A; git commit -a -m "upgrading
standby ramp"; git push origin master
[master 88562d8] installing ramp
 1 file changed, 1 insertion(+), 1 deletion(-)
Counting objects: 11, done.

```

```
Delta compression using up to 24 threads.
Compressing objects: 100% (5/5), done.
Writing objects: 100% (6/6), 530 bytes | 0 bytes/s, done.
Total 6 (delta 3), reused 0 (delta 0)
To ssh://git@bitbucket.rbbn.com:7999/ems/rbbn-cnf-gitops-ramp-svt.git
    01f6ef4..88562d8  master -> master
[ssequeira@cli-blr-2 jenkinsbuild-dev]$
```

9. Check the status of the RAMP Standby instance. For more information, refer to [Check RAMP Status](#).

Before you proceed, ensure that the RAMP Standby instance is running.

10. Ensure the SSH keys, `authorized_keys`, and `known_hosts` for the insight user on the RAMP Standby instance are the same as before the upgrade.
11. On the RAMP Active instance, configure GR parameters. For more information, refer to [Configuring RAMP GR](#).

There may be Performance Management (PM) collection data loss for around 15 minutes while configuring GR.

In addition, the PM data collected by the Standby RAMP instance while recreating the RAMP Active instance will be lost while configuring RAMP GR. During upgrade, data sync does not occur between the RAMP Standby and Active instance.

12. The status of the Active and Standby instances may show as offline on the upgraded RAMP. Rediscover both active and Standby RAMP instances. For more information, refer to [How to Rediscover the localhost](#).
13. To ensure password-less SSH connection is working from the RAMP Active to Standby instance and vice versa, refer to [Establish RAMP CNF Active-Standby Instance Passwordless Connection](#).

Post-Upgrade Procedure

After you perform an upgrade, perform post-upgrade procedures. For more information, refer to [RAMP CNF - Post-Upgrade Procedures](#).

RAMP CNF - Post-Upgrade Procedures

After successfully upgrading Ribbon Application Management Platform (RAMP), complete the following procedures, as needed, before using RAMP.

Step	Procedure	Mandatory (M)/ Optional (O)
1	How to Rediscover the localhost	M
2	Clear the Client Java Cache and Browser Cookies After Upgrade	M

Step	Procedure	Mandatory (M)/ Optional (O)
3	Install PSX Manager on RAMP	O
4	Deploy MNP Services	O
5	Exported PM CSV Files column Order Post upgrade Rollback Procedure	O

Post-Upgrade Procedures for RAMP

Note

If upgrading from a pre-22.12 RAMP release, you must discover all the nodes after completing the upgrade.

After successfully upgrading Ribbon Application Management Platform (RAMP), complete the following procedures, as needed, before using RAMP.

Step	Action
1	How to Rediscover the localhost
2	Clear the Client Java Cache and Browser Cookies
3	Install PSX Manager on RAMP
4	Deploy MNP Services
5	(Optional) If the SBC image files were previously copied over, restore the files to <code>/opt/sonus/ems/image_upgrade</code> : <pre>scp -r admin@<remote_ip>:/opt/sbc_image_bkup/* /opt/sonus/ems/image_upgrade/ chown -R insight:insight /opt/sonus/ems/image_upgrade/</pre>
6	(Optional) After an upgrade, you can rollback the column order for the exported PM CSV files. For more information, refer to Exported PM CSV Files column Order Post upgrade Rollback Procedure.

Step	Action
7	Note This procedure is mandatory whenever the RAMP is upgraded from any version less than 24.06 especially when RAMP utilizes LDAPS authentication. (Optional) Disable Endpoint Notification for LDAP over SSL/TLS connections. For more information, refer to Disable Endpoint Notification for LDAP Over SSL/TLS Connections.
8	For customers using the GSX, refer to Legacy Device Management .
9	Note Applicable only if your active directory is already configured. To reconfigure the active directory for: • Non-cloud RAMP (KVM, VMWare, and ROHOS), refer to Accessing RAMP VNF Using Active Directory. • Cloud RAMP, refer to Reconfiguring Active Directory.
10	After you upgrade to the RAMP 24.12, by default the node level postpaid reports are disabled. For more information, refer to Set Up Reporting for Post-Paid Billing .

Note

After an upgrade, the SBC Edge nodes take approximately five minutes to become online after an upgrade.

Clear the Client Java Cache and Browser Cookies After Upgrade

After performing an upgrade to a new version of Ribbon Application Management Platform (RAMP), each RAMP user must clear their Java cache to prevent the display of cached pages from the previous version. Similarly, users must also clear browser cookies to ensure there is no carryover from an earlier version of RAMP.

Prerequisite

Close all browsers before beginning the procedure.

Start

To clear the Java cache on Microsoft Windows:

1. Open the Windows **Control Panel**.
2. Select **Java** to open the **Java Control Panel**.

3. On the **General** tab under **Temporary Internet Files**, click **Settings**.
The **Temporary File Settings** window opens.
4. Click **Delete Files**.
The **Delete Files and Applications** window opens.
 - a. Check **Trace and Log Files** to delete trace and log files.
 - b. Check **Cached Applications and Applets** to delete applications and applets.

It is not necessary to select the **Installed Applications and Applets** check box.

- c. Click **Ok** to save the changes and close the **Delete Files and Applications** window.
5. Click **Ok** on the **Temporary File Settings** window to save the changes and close the window.
6. Click **Ok** on the **Java Control Panel** window to clear the cache.

The procedure to clear browser cookies depends on the type of browser. Check the documentation for the browser for specific steps.

Migrating to RAMP

In this section

- [Migrate EdgeView to RAMP](#)
- [Migrate Insight EMS to RAMP](#)

Perform the procedures in this section to migrate from EMS or EdgeView to The Ribbon Application Management Platform (RAMP).

Migrate EdgeView to RAMP

Use this procedure to migrate the EdgeView service to the Ribbon Application Management Platform (RAMP). Migration from EdgeView to the RAMP is done in phases. The first phase is to install the RAMP 23.09 or 23.12 version and then create users based on the users on EdgeView. After you create users and resource groups based on the existing EdgeView configuration, select all EdgeMarc devices from EdgeView and push the configuration specifying the RAMP FQDN or IP as the new management application.

Perform the following steps to migrate the devices and users from the EdgeView to the RAMP.

Step	Action
1	Manually install RAMP based on your deployment model, refer to Installation and Upgrade Guide .
2	Deploy the EdgeView service on RAMP. For more information, refer to Deploy Optional Services on RAMP .

Step	Action
3	Select all EdgeMarc devices on EdgeView and perform the push configuration specifying the RAMP FQDN or IP as the new management application. The configuration file to push for re-directing devices to the RAMP IP address using the instructions above. Configuration <pre>FILE:/etc/config/evagent.conf EDGEVIEW_HOST="<RAMP IP/FQDN>"</pre> Change < RAMP IP/FQDN > to the customer actual IP/FQDN of RAMP. For more information, refer to Perform Actions on EdgeMarc.
4	Create resource groups based on EdgeView collections, and map the EdgeMarc devices accordingly. For more information, refer to Work with Resource Groups.
5	Add users on RAMP based on the users on EdgeView and map the resource groups created earlier to the users accordingly. For more information, refer to: • Add Users • Add User Groups

Migrate Insight EMS to RAMP

In this section:

- [Overview](#)
- [Prerequisites](#)
 - [What is Not Migrated](#)
 - [Limitations](#)
- [EMS to RAMP Migration Notes](#)
- [Supported Scenarios](#)
- [High-Level Steps](#)
- [Frequently Asked Questions](#)
- [Support/Questions](#)
- [MOP Creation Instructions](#)
 - [Download Script](#)
 - [Install and Follow the Script Instructions](#)

Overview

Customers/partners can migrate the Insight EMS to the Ribbon Application Management Platform (RAMP) using the guidance provided in this document. The objective of this documentation is to outline the general requirements, limitations and steps involved in this migration process, as well as how to use the Ribbon-provided tool to automatically generate a scenario-specific Method Of Procedure (MOP) that you will follow to complete the EMS to RAMP migration. As noted below, the config drive(s) for KVM and VMWare RAMP installation is/are created as part of this process for use during the deployment of RAMP.

Note

You can migrate the following Insight EMS versions to RAMP:

- 13.x
- 14.x
- 15.x

Note

Post migration if the mgmt1 is configured, you must manually update the management client to secondary IP to manage the nodes with secondary management client IP.

Prerequisites

Ensure the following prerequisites are in place prior to starting the migration from the EMS to RAMP.

1. A remote server is available to store the backup.
2. Required resources (vCPU, disk space, memory) for a RAMP deployment are available.
3. A localhost is registered on the EMS before initiating the migration to RAMP.
4. **Take note of all Nodes that are offline before doing the migration.**
 - a. Try to discover them manually before doing migration.
 - b. If you could not discover a node, it will be offline post-migration and you will need to bring it up manually.
 - c. This also saves time during maintenance window as there is no requirement to fix the offline nodes.
5. If you previously changed the EMS GUI password using `changePassword.py` script, then synchronize the credentials to PSX by using the **Synchronize** option in the **Users & Roles** page before migrating to RAMP.
6. Download the Users and Roles reports to the local workstation since they are not supported on RAMP.
7. Licensing: Contact your Account Team if you are using Network Wide Licensing (NWL) licenses on EMS. RAMP supports the use of NWL licenses, but does not support Usage Reporting for NWL licenses.
8. The restore script sets the postgres user password back to default. You may use an EMS RAMP backup with passwords.

What is Not Migrated

- Do not migrate Performance Management (PM), CSV and parquet files directly from the EMS to RAMP.
 - Export the CSV files to a third-party OSS before starting the migration, if needed.
- System files and modified configuration files (e.g., crontab/logrotate) are not migrated,

- Back up these changes before initiating the migration.
- Upgrade images of devices stored in EMS and Scheduled upgrades are not migrated.
 - Upload the upgrade image to RAMP post-migration.
- Devices stored in the EMS and scheduled upgrades are not migrated.
- Any configuration for Radius authentication on the EMS is not migrated. Customers using Radius must re-configure the data on RAMP post-migration.

Limitations

1. The RAMP does not support pre-11.0 SBC Edge devices. Upgrade the SBC Edge device to 11.0 or later and post the migration to RAMP to dynamically register the device.
2. Any requirements for migrating Network-Wide Licensing to another License Type is handled separately.
3. The RAMP does not support multiple interfaces.
4. The RAMP does not support Trap Forwarding Profiles that contain non-alphanumeric characters. If this is present on EMS, update the Profile name to remove non-alphanumeric characters before migrating to RAMP.
5. The AWS RAMP does not support management of non-AWS nodes.
6. The AWS requires retained Hostname and IP address values.
7. The RAMP Platform Type (VMware, KVM, AWS, OpenStack) should match EMS Platform Type.
8. The RAMP Deployment Mode (Standalone, GR, GR with Auto-Switchover) should match EMS Deployment Model.
9. For OpenStack, if new IP address(es) are used for the RAMP, this requires manual action on each OpenStack SBC/PSX Instance to re-register to the new address value(s).
10. For OpenStack, migration is supported, but the Auto creation of the MOP as outlined below is not supported.
11. Nodes should not be managed by EMS and RAMP at the same time.
12. Migration from non-JITC EMS to JITC RAMP is not supported.
13. Ensure to review the [RAMP Release Notes and Documentation](#) to confirm the following support:
 - a. Support for the current managed nodes/versions
 - b. API version support (if applicable)
 - c. Support of the Cipher and Key Algorithm versions (RAMP does not support some of the weaker versions)
14. This process does not utilize the 24.03 Feature AFM-4303 which introduces OVA Template Customization for VMWare.
15. If New IP Address(es) are used for RAMP the following limitations apply:
 - a. Network modifications may be required to allow the new IP value(s) on RAMP to properly interact with Managed Nodes or Northbound OSS platforms.
 - b. For Devices which have Automatic or Dynamic Registration, action will be required on the Device to reflect the new RAMP IP(s). For more information, refer to [Registering Devices on RAMP](#).
 - c. Analytics: If you are configured for mitigation from Analytics on the PSX via the EMS/RAMP changes to reflect the new RAMP IP address are required. For more information, refer to [Configuring Ribbon PSX Devices](#).
16. IPv6 address migration is supported, but the Auto creation of the MOP as outlined below is not supported using IPv6 addresses.

EMS to RAMP Migration Notes

During the migration of data from EMS to RAMP, take note of the following:

- The alarms in the EMS are not migrated to RAMP.
- Inventory Reports in EMS are not migrated to RAMP.
- The Node/Cluster status history data in Cluster Management of EMS are not migrated to RAMP.
- Call trace reports, Call history reports in EMS will not be migrated to RAMP.
- The Fault Manager administration settings in EMS are not migrated to RAMP.
- The EMS User and IP locks feature is not supported in RAMP.

- Password retention:
 - The EMS insight Linux user password is not retained as part of migration.
 - The EMS admin Linux user password is not retained as part of migration. Use the RAMP password.
 - The EMS admin UI user password is not retained as part of migration. Use the default RAMP password.
 - The EMS UI users are migrated to RAMP, but due to strict password rules on RAMP the UI users will be enforced to set a new password as per RAMP on the first login.
- Post-migration as admin user update the roles of non-admin users and enable the access to Device Management (Devices, Resource Group, Inventory).
- Post-migration the associated count in License Association screen of License Management is shown as zero and status will be in ready state for the migrated NWDL licenses.
- If a User belongs to multiple user groups with varying permissions for each user group in EMS, such a user's permission post-migration will not be guaranteed to have correct role permission.
 - So it is advised to provision a user to a user groups which have identical roles in EMS pre-migration.
 - Eg : Suppose a user "admin" is associated with more than 1 User groups and is one user group has Login Permission role and another user group has Login Permission role disabled, there is no guarantee that user "admin" will have RAMP Login permission post-migration. Hence, we should not have different role permissions for a user who belongs to multiple user groups.
- IpTables rules are not restored post-migration, hence the EMS and RAMP maintain their own set of Iptables rules. You must reconfigure the required ports post-migration.
- /opt/rbbn/ems/conf/enableEmailNotification.sh <EMAIL Server IP> should be used to re-enable FM email notification if configured.
- A PM Collection Profile that is not associated with any node is not migrated.
- By default, RAMP uses IP addresses in the "172.xxx" range for Docker and other applications. If this will conflict with your existing Network Infrastructure, contact your Account Team to arrange for assistance to overcome this conflict.
- All SBC 7000 PM-related configurations are not migrated ex: templates, reports, Thresholding, collection profiles
 - The Collection Profile for an SBC 7000 node is changed to "Default SBX5K SFTP Profile" in Collection Assignments page post-migration.
 - The Export Profile for an SBC 7000 node is changed to "Default SBX5K Profile" in Export Assignments page post-migration.
 - It is mandatory to enable the SBC 7000 Export Profile post-migration.
- Any certificates in used in Observability -> Lawful Intercept -> Mediation Server for Lawful Interface are not migrated.
- To manage SBC Edge devices with Ribbon Application Management Platform (RAMP), you must deploy the EdgeView (EV) service on RAMP. You may also need System Registration on RAMP, refer to [System Registration](#).
- If STI/IDH devices are configured on the EMS, then install the STI Manager/IDH Manager application on RAMP after the migration. For more information, on STI refer to [Migrating STI Manager from Insight EMS to RAMP](#) and for IDH, refer to [Migrating Identity Hub Manager from Insight EMS to RAMP](#).
- For customers having GSX, after an upgrade and migration, before discovering GSX, run the script: `/opt/sonus/ems/conf/updateSystemCryptoPolicy.sh` . For more information, refer to [Legacy Device Management](#).
- After you migrate to the RAMP 24.12, by default the node level postpaid reports are disabled. For more information, refer to [Set Up Reporting for Post-Paid Billing](#).

Supported Scenarios

Refer to the "Migration Notes" table in the latest [RAMP Release Notes](#) for the supported deployment models.

Example

Migration Notes

The following migration paths are supported in this release.

Platform	EMS Release
KVM	15.X, 14.x, 13.x
VMware	15.X, 14.x, 13.x
OpenStack	15.X, 14.x, 13.x
AWS	15.X, 14.x, 13.x

Customers can either retain IP address and hostname values or use new values. Items that impact the procedure include:

Decision Point	Limitations	Impact on Procedure
RAMP Deployment Model (Standalone, GR, GR with Auto-Switchover)	RAMP Deployment Mode should match EMS Deployment Model.	The GR allows for the migration to take place for 1 EMS Node while the other EMS Node Remains available. For GR with Auto-Switchover, 3 etcd Nodes are required, which are in addition to and separate from the RAMP Nodes.
Retained or new Hostname Value(s)	Must use valid RAMP hostname syntax.	If the hostname does not change, the ssh keys for admin/insight users are restored. If the hostname changes, the MOP includes the manual steps to backup/restore the ssh keys.
Retained or new IP Address Value(s)	See the Limitations section above if New IP Address(es) are used for RAMP.	New IP address values allow for building the RAMP node in advance of the migration, but retaining IP address values allow for easier transition for managed nodes and 3rd party OSS Interactions such as Trap Forwarding or Provisioning.
Types of Nodes Managed, Software Version of Nodes	See the Limitations section above.	Edge Devices will require the deployment of the EdgeView service. NWDL license support is dependent on Node Type and Software Version.

Decision Point	Limitations	Impact on Procedure
Platform Type	VMware, KVM, AWS, OpenStack Only. RAMP Platform Type should match EMS Platform Type.	AWS requires retained Hostname and IP address values. NOTE: OpenStack Auto-MOP creation is not supported, but Professional Services can provide assistance with MOP Creation for OpenStack customers.

High-Level Steps

For Standalone when using new IP address

1. Pre-Migration:
 - a. Install the RAMP instance on a new VM.
 - b. Verify the sanity of the EMS.
 - c. Take RAMP backup of the EMS.
2. Migration Maintenance Window:
 - a. Stop Insight on EMS Node
 - b. Restore the EMS backup onto the RAMP instance.
 - c. Perform Post-Install Steps on RAMP and Validate functionality on RAMP.

For Standalone when using same IP address

1. Pre-Migration:
 - a. Verify the sanity of the EMS.
 - b. Take RAMP backup of the EMS.
2. Migration Maintenance Window:
 - a. Power down the EMS VM.
 - b. Install the RAMP instance on a new VM.
 - c. Restore the EMS backup onto the RAMP instance.
 - d. Perform Post-Install Steps on RAMP and Validate functionality on RAMP.

For GR when using new IP addresses

1. Pre-Migration:
 - a. Install RAMP1 and RAMP2 nodes with new IP addresses and Hostnames.
 - b. Verify the sanity of the EMS.
 - c. Take RAMP backup of the active EMS.
2. Migration Maintenance Window #1:
 - a. Teardown GR on EMS Nodes.
 - b. Stop Insight on the EMS1 Node.
 - c. Restore the EMS backup onto the Source/Active RAMP (RAMP1).
 - d. Stop Insight on the EMS2 Node.
 - e. Perform Post-Install Steps on RAMP1 and Validate RAMP functionality on RAMP1.
3. Migration Maintenance Window #2:
 - a. Perform Post-Install Steps on RAMP2
 - b. Establish GR for the RAMP nodes
 - c. Install RAMP-BASE-GR license

For GR when using same IP addresses

1. Pre-Migration:
 - a. Verify the sanity of the EMS.

- b. Take RAMP backup of the active EMS.
2. Migration Maintenance Window #1:
 - a. Teardown GR on EMS Nodes.
 - b. Stop Insight on the EMS1 Node and power down the EMS1 VM.
 - c. Install Source/Active RAMP (RAMP1).
 - d. Stop EMS2 and restore the EMS backup onto RAMP1
 - e. Perform Post-Install Steps on RAMP1 and Validate RAMP functionality on RAMP1.
3. Migration Maintenance Window #2:
 - a. Power down the EMS2 VM and install Target RAMP (RAMP2).
 - b. Perform Post-Install Steps on RAMP2.
 - c. Establish GR for the RAMP nodes.
 - d. Install RAMP-BASE-GR license

Frequently Asked Questions

- What if my migration scenario is not listed in the Supported Scenarios section above?
 - **Answer:** Contact your Account Team who can consult with Professional Services for guidance.
- Since Node-Locked licenses are tied to the EMS Hostid, do I need to regenerate licenses for RAMP?
 - **Answer:** No, Node-Locked licenses installed on the EMS are migrated to RAMP. You only need to generate the new RAMP-BASE or RAMP-BASE-GR licenses with the new RAMP Hostid(s).
- Can I just install a RAMP node and register my nodes with RAMP?
 - **Answer:** For smaller networks, this is a possibility, but there are limitations. For example, it is not recommended to have a node managed by both EMS and RAMP at the same time, and you must regenerate any licenses with the new RAMP information. Please contact your Account Team if you consider this possibility.

Support/Questions

If you have questions on the migration process or errors during the the script operation or MOP creation, please email: RAMP.Auto-MOP.Support@rbbn.com.

MOP Creation Instructions

Follow the instructions below to create the auto-MOP and in some cases, the config drive file(s) required for installing RAMP.

Download Script

1. From the [Ribbon Support Portal](#), select "Tools & Services" from the menu bar, and then select "Go to EMS to RAMP Migration."
2. Access the EMS to RAMP Migration webpage via the Ribbon Support Portal.

[Example](#)

EMS to RAMP Migration



Step 1: Audit for Migration data

expand for instructions

Step 2: Auto MOP Generation + config-drives

expand to execute Step 2

- Expand the Step 1 instructions and click the button to download the script.

Example

Step 1: Audit for Migration data

expand for instructions

EMS Audit Script Download

Download the audit script and run on the EMS. Answer all questions. This will generate a file that will be used in step 2.

Install and Follow the Script Instructions

- Place this script on each EMS node in any directory that allows issuing the script (e.g., `/tmp`).
- As root user, use the `chown` and `chmod` commands to set the ownership of the file to `root:root` and give full permissions.

Example

```
chown root:root EMS_RAMP_Migration.sh
chmod 777 EMS_RAMP_Migration.sh
```

- Run the script as root user:
 - Standalone EMS nodes:

```
./EMS_RAMP_Migration.sh -c
```

- b. HA or GR EMS nodes:

On the Source/Active EMS:

```
./EMS_RAMP_Migration.sh -c
```

On the Target/Standby EMS:

```
./EMS_RAMP_Migration.sh -t
```

4. On the Standalone and Source EMS, answer the following questions when prompted:

Note

For the Target EMS, this script is run just to gather server-specific data such as 'Time Zone' and 'NTP Server'. Thus, you are only prompted for 'Customer Name' and 'Customer Environment.'

- a. **Customer Name** (Do not use spaces)
 - b. **Environment:** Lab, Production, etc. (Do not use spaces)
 - c. **Platform Type** (VMware, KVM, AWS)
 - d. If you want to change hostnames on RAMP
 - i. You are prompted for the new hostname(s).
 - e. If you want to change IP addresses on RAMP
 - i. You are prompted for the new IP address(es), Gateway Value(s), Netmask value(s).
5. Once the script completes, the text file "`<CustomerName>-<Environment>-<Date&Time>.txt`" is produced.
- a. Save the file to your local drive.
6. (GR EMS only) If you run the script for a GR EMS, copy the resulting text file from the second EMS to the first EMS in the same directory where the script was run.
- a. On the first EMS, run the script again with the "`-m`" option to merge the two files:


```
./EMS_RAMP_Migration.sh -m
```
 - b. You are prompted for the two file names.
 - c. Once the script completes, the text file "`<CustomerName>-<Environment>-<Date&Time>.txt-GR.txt`" is produced.
 - i. Save the file to your local drive.
7. By Default, the MOP will be built to use RAMP 24.09. If you want to instead use RAMP 23.12 or 24.03 or 24.06 manually edit the text file and modify the line "RAMP Version = 24.09" to reflect either RAMP 23.12 or 24.03, or 24.06.
8. Move on to auto-MOP step 2.

Step 2: Auto MOP Generation + config-drives

expand to execute Step 2

Provide a session name

Step 2a - Provide a session name and press **Enter**

Step 2b - You will be prompted to upload the generated file from Step 1

Step 2c - Download buttons for doc and config-drives display

Step 2 Instructions

1. Provide a session name (This is simply a free text string field to identify the customer and environment). The prompt allows for an upload of the text file generated from the EMS_RAMP_Migration script.
NOTE: Always use a text file generated from the latest version of the EMS_RAMP_Migration script – files created from earlier versions may not process correctly in Step 2.

Step 2: Auto MOP Generation + config-drives

expand to execute Step 2

Upload EMS 2 RAMP CIQ



Drag and drop file here

Limit 200MB per file • TXT

Browse files

Step 2a - Provide a session name and press **Enter**

Step 2b - You will be prompted to upload the generated file from Step 1

Step 2c - Download buttons for doc and config-drives display

2. Upload the text file (Drag and drop or browse to input the text file). This generates the auto-MOP; and in some cases, a config drive is created for use during the deployment of RAMP.

Here is an example for a GR on VMware:

Step 2: Auto MOP Generation + config-drives

expand to execute Step 2

Step 2a - Provide a session name and press **Enter**

Step 2b - You will be prompted to upload the generated file from Step 1

Step 2c - Download buttons for doc and config-drives display

UploadedFile(id=12, name='DEMO-Lab-20231005-GR.txt', type='text/plain', size=4223)

V14

Use the buttons to download files

GR

DEMO-Lab EMS-GR To RAMP-GR MoP V1.0.docx

RAMP1.configDriveImgDeployment.iso

RAMP2.configDriveImgDeployment.iso

3. Download the MOP and config drive files.

Installing etcd

The software installation of the Services VMs consists of creating each VM and allowing each VM's database member to re-synchronize with the rest of the database.

Throughout the installation procedures, the following naming conventions apply:

- **appetcd1**, **appetcd2** and **appetcd3** represent the three Application Services VMs (referred to as Services VMs).

You can replace those names with host names or any other specific names you choose, as long as you maintain consistency throughout the steps. However, Ribbon recommends that you rename the files to the above naming conventions when copying the files to the host server to make it easier to follow the procedure examples.

Additionally, to distinguish one release version from another, Ribbon recommends that you include the release version in the file name. For example:

- **APPETCD1_ [release version]**
- **APPETCD2_ [release version]**
- **APPETCD3_ [release version]**

- [Installing etcd on Kubernetes](#)
- [Installing etcd on KVM](#)
- [Installing etcd on OpenStack](#)
- [Installing etcd on VMware](#)

Installing etcd on Kubernetes

Prerequisites

- Three free IP addresses are available to allocate to the etcd instances.
- Ensure the platforms use RCP 5.4.3 and/or OCP RH-openshift 4.10.18 or later versions.
- Review [RAMP etcd System Requirements](#) to ensure your environment has the necessary resources and prerequisite software available.

Start

1. Log on to the Ribbon Support portal and download the `He`lm` chart for etcd. For more information on using the portal, refer to [Download Files from Ribbon Support Portal](#).
2. Log on to OpenShift Jumpserver and untar the `He`lm` chart:

```
tar -xvf <name of the Helm chart>.tar
```

3. Change the directory:

```
cd etcd/
```

4. Edit the values in the `yaml` file:

```
vi values.yaml
```

For more information on etcd parameters, refer to [etcd Parameters](#).

5. Install the `He`lm` chart after editing the values in the `.yaml` file:

```
helm install <deployment name> --values values.yaml .
```

Example

```
## @section Global parameters
```

```

## Please, note that this will override the image parameters, including
dependencies, configured to use the global value
##
global:
  ## @param global.imageRegistry Containers image registry
  ##
  imageRegistry: "artifact2.eng.sonusnet.com"
  ## @param global.imagePullSecrets [array] Global Docker registry secret names as
  an array
  ## E.g.
  ## imagePullSecrets:
  ##   - name: myRegistryKeySecretName
  ## Note: for backwards compatibility, directly specifying the secrets as a list
  of strings without the name: attribute is also supported, but not recommended
  ##
  imagePullSecrets: ["sanramp-imagecred"]
  ## @param global.imagePullSecretsTemplate [array]
  ## Template strings to evaluate to existing secret to use to pull images, for
  example: name: "{{.Release.Name }}-imagecred"
  ##
  imagePullSecretsTemplate: []
  ## @param imageCredentials Create image pull credentials
  ##
  imageCredentials:
    name: "ssequeira-8"
    registry: artifact2.eng.sonusnet.com
    username: ssequeira
    password:
eyJ2ZXIiOiIyIiwidHlwIjoIiSldUIiwiYWxnIjoIulMyNTYiLCJraWQiOiJ0b2Z0emxGZGtnSjdaWfZnRn
RTTm94RzBLMTE3ZEZldEVaVXd5YVg3a2xvIn0.eyJzdWIiOiJqZnJ0QDAXY2RxYnJwejljYzclMXFnemI5
bTlxaHB1XC91c2Vyc1wvc3NlcXVlaXJhIiwic2NwIjoibWVtYmVyLW9mLWdyb3Vwc3pyZWfKZXJzIiwiaXNz
VkIjoiamZydEAAQIiwiaXNzIjoiamZydEAAwMWNkcWJycHo5Y2M3NTFfXz3piOW0yMWhwZVwvdXNlcnNcL3Nz
ZXF1ZWlyYSIsImV4cCI6MTczNzYwMTM0MiwiawF0IjoxNzA2MDY1MzQyLCJqdGkiOiJmZWFlNjI0ZS0yMz
IwLTRhZDEtOGM5Mj0xMzUyNzI5MDc0NzkiZjQ.Z_E60050KSvANFBXMoQeJBQLBSr3taxE1xhZQmDWQx6Yj
0u7pW1rt6-P6kaECuSFf7X-
xqBxqAKUr8TBbzq20n8DyrQoCfuqAv5UcD77TAE4H1290p1HhHtcs3f7f10dwiEhNDA932X0EGAIATHPI1
yWqx3qcaD849FbPq18bZFWNzXYBNkhABZ4g_gn6j8IUEj5yjdBNXn_b3JFzIfvH6hwyXBgaMCXDtSzbH6g
jvMMLUq9lC9GTLxv7qhnnqB5uMRumlVuv4X0BUVKtFDsk3EEefQFV4I-
xsFd66iEkR03qI7s063Xsopfoq_KipwUPP5pSsPHks3B7NyN2dqxiA
  ## @param global.serviceAccount to use for pods
  ##
  serviceAccount:
    ## @param global.serviceAccount.name Name of the service account to use
    ##
    name: ""
  ## @param global.storageClass Global StorageClass for Persistent Volume(s)
  ##
  storageClass: ""
  ## Cert-manager information to use in the csi-driver volume
  ##
  certManager:
    ## @param global.certManager.enabled Switch to enable the use of cert-manager
    to manage certificates

```

```

##
enabled: true
issuer:
  ## @param global.certManager.issuer.name The Issuer name to sign the
certificate request
  ##
  name: "cross-cluster-ca-selfsigned-clusterissuer"
  ## @param global.certManager.issuer.kind The Issuer kind to sign the
certificate request. Can be "Issuer" or "ClusterIssuer"
  ## See https://cert-manager.io/docs/concepts/issuer/ for more information
  ##
  kind: "ClusterIssuer"
## @param global.ns_uuid Global NS UUID
##
ns_uuid: "ns_uuid"
## @param global.cnf_uuid Global CNF UUID
##
cnf_uuid: "cnf_uuid"
## @param global.cnfc_uuid Global CNFC UUID
##
cnfc_uuid: "cnfc_uuid1"
## @param global.kubernetesPlatform K8s platform type: "oc" or "robin"
##
kubernetesPlatform: ""
## @param global.obs parameters
##
obs:
  ## @param global.obs.image image parameters
  ##
  image:
    ## @param global.obs.image.repository observability agent image name
    ##
    repository: "ccs-docker-prod-virtual/rbbn_telemetry_collector"
    ## @param global.obs.image.tag observability agent image tag
    ##
    tag: "3.1.1"
    ## @param global.obs.image.pullPolicy observability agent image pull policy.
Defaults to 'Always' if image tag is 'latest', else set to 'IfNotPresent'
    ##
    pullPolicy: IfNotPresent
  ## @param global.obs.logPersistentVolumeStorage settings for log PVC
  ##
  logPersistentVolumeStorage:
    ## @param global.obs.logPersistentVolumeStorage.request Size of the PVC
storage request
    ##
    request: 20Gi
  ## @param global.obs.logs parameters
  ##
  logs:
    ## @param global.obs.logs.telemetry log telemetry config
    telemetry:

```



```

    ## @param global.obs.logs.telemetry.topic telemetry logs will be sent to
this Kafka topic
    topic: rbbn-otel-agent
    ## @param global.obs.logs.backendServers log backends
    ##
    backendServers: {}
    ## @param obs.logs.backendServers.elasticsearch elasticsearch backend
    ## Warning: username and password represent the name of the ENV variable
name
    ## that contains the username and password from the secret
    # elasticsearch:
    #   - endpoint: <elasticsearch server address>:443
    #     auth: True
    #     username: ELASTICSEARCH_USER
    #     password: ELASTICSEARCH_PASSWD
    #     index: <filebeat index>
    ## @param obs.logs.backendServers.kafka kafka backend
    ##
    # kafka:
    #   - endpoint: <kafka server address>:<kafka port>
    #     sslCert: KAFKA_CERT
    #     sslKey: KAFKA_KEY
    #     sslCa: KAFKA_CA
    ## @param global.obs.logs.elasticsearchSecretName name of common
elasticsearch credentials secret
    ##
    elasticsearchSecretName: ""
    ## @param obs.logs.kafkaSecretName Name of secret containing Kafka
environment variables
    ## Evaluated as a template, for example: "{{ .Release.Name }}-elasticsearch-
user-creds"
    #
    elasticsearchSecretNameTemplate: ""
    ## @param global.obs.logs.elasticsearchSecretName name of common kafka
credentials secret
    ##
    kafkaSecretName: ""
    ## @param obs.logs.kafkaSecretName Name of secret containing Kafka
environment variables
    ## Evaluated as a template, for example: "{{ .Release.Name }}-kafka-user-
creds"
    ##
    kafkaSecretNameTemplate: ""

    ## @param global.prometheusRule Prometheus alerting rules
    ##
    prometheusRule:
    ## @param global.prometheusRule.create Specifies whether a PrometheusRule
resource should be created
    ##
    # create: false
    ## @param global.prometheusRule.labels Specify additional labels so the
Prometheus instance can discover the rules

```

```

##
labels: {}

## @param global.customizedResourcePrefix template definitions for resource name
prefixes
##
customizedResourcePrefix:
  servicePrefixTemplate: ""
  configmapPrefixTemplate: ""

persistence:
  ## @param global.persistence.annotations Annotations to add to the
  PersistentVolumeClaims
  ##
  annotations: {}

## @param global.terminationMessagePolicy Container termination message policy
## https://kubernetes.io/docs/tasks/debug/debug-application/determine-reason-
pod-failure/
terminationMessagePolicy: "FallbackToLogsOnError"
## @param global.tolerations [array] Tolerations for pod assignment
## Ref: https://kubernetes.io/docs/concepts/configuration/taint-and-toleration/
##
tolerations: []

## @section Common parameters

## @param kubeVersion Force target Kubernetes version (using Helm capabilities if
not set)
##
kubeVersion: ""
## @param nameOverride String to partially override etcd.fullname template (will
maintain the release name)
##
nameOverride: ""
## @param fullnameOverride String to fully override etcd.fullname template
##
fullnameOverride: ""
## @param commonLabels [object] Labels to add to all deployed objects
##
commonLabels: {}
## @param commonAnnotations [object] Annotations to add to all deployed objects
##
commonAnnotations: {}
## @param clusterDomain Default Kubernetes cluster domain
##
clusterDomain: cluster.local
## @param extraDeploy [array] Array of extra objects to deploy with the release
##
extraDeploy: []

## @section roles parameters
##

```

```

roles:
  ## @param roles.create Enable/disable Role and RoleBinding creation. If set to
  ## false, the ServiceAccount passed in global will need the following rules:
  ## If using a NodePort service:
  ## - apiGroups: [""] # "" indicates the core API group
  ##   resources: ["services"]
  ##   verbs: ["get"]
  ## If using persistence:
  ## - apiGroups: [""]
  ##   resources: ["persistentvolumeclaims"]
  ##   verbs: ["get", "list", "delete", "deletecollection"]
  ##
  create: false

## Enable diagnostic mode in the deployment
##
diagnosticMode:
  ## @param diagnosticMode.enabled Enable diagnostic mode (all probes will be
  ## disabled and the command will be overridden)
  ##
  enabled: false
  ## @param diagnosticMode.command [array] Command to override all containers in
  ## the deployment
  ##
  command:
    - sleep
  ## @param diagnosticMode.args [array] Args to override all containers in the
  ## deployment
  ##
  args:
    - infinity

## @param imageRegistryPath Containers image repository path in the registry
##
imageRegistryPath: "/dockerhub-docker-remote"

## @section etcd parameters

## etcd image version
## ref: https://console.cloud.google.com/gcr/images/etcd-development/GLOBAL/etcd
## ref: https://hub.docker.com/r/bitnami/etcd/tags/
## @param image.repository etcd image name
## @param image.tag etcd image tag
## @param image.pullPolicy etcd image pull policy
##
image:
  repository: bitnami/etcd
  tag: 3.5.13
  ## Specify a imagePullPolicy
  ## Defaults to 'Always' if image tag is 'latest', else set to 'IfNotPresent'
  ## ref: https://kubernetes.io/docs/user-guide/images/#pre-pulling-images
  ##
  pullPolicy: IfNotPresent

```

```

## Set to true if you would like to see extra information on logs
##
debug: false
## kubectl image (used for init and cleanup)
## ref: https://hub.docker.com/r/bitnami/kubectl/tags/
## @param kubectl.image.repository kubectl image name
## @param kubectl.image.tag kubectl image tag
##
kubectl:
  image:
    repository: bitnami/kubectl
    tag: 1.30.1
## Authentication parameters
##
auth:
  ## Role-based access control parameters
  ## ref: https://etcd.io/docs/current/op-guide/authentication/
  ##
  rbac:
    ## @param auth.rbac.create Switch to enable RBAC authentication
    ##
    create: false
    ## @param auth.rbac.allowNoneAuthentication Allow to use etcd without
    configuring RBAC authentication
    ##
    allowNoneAuthentication: true
    ## @param auth.rbac.rootPassword Root user password. The root user is always
    `root`
    ##
    rootPassword: ""
    ## @param auth.rbac.existingSecret Name of the existing secret containing
    credentials for the root user
    ##
    existingSecret: ""
    ## @param auth.rbac.existingSecretPasswordKey Name of key containing password
    to be retrieved from the existing secret
    ##
    existingSecretPasswordKey: ""
  ## Authentication token
  ## ref: https://etcd.io/docs/latest/learning/design-auth-v3/#two-types-of-tokens-simple-and-jwt
  ##
  token:
    ## @param auth.token.type Authentication token type. Allowed values: 'simple'
    or 'jwt'
    ## ref: https://etcd.io/docs/latest/op-guide/configuration/#--auth-token
    ##
    type: jwt
    ## @param auth.token.privateKey.filename Name of the file containing the
    private key for signing the JWT token
    ## @param auth.token.privateKey.existingSecret Name of the existing secret
    containing the private key for signing the JWT token
    ## NOTE: Ignored if auth.token.type=simple

```

```

    ## NOTE: A secret containing a private key will be auto-generated if an
    existing one is not provided.
    ##
    privateKey:
      filename: jwt-token.pem
      existingSecret: ""
    ## @param auth.token.signMethod JWT token sign method
    ## NOTE: Ignored if auth.token.type=simple
    ##
    signMethod: RS256
    ## @param auth.token.ttl JWT token TTL
    ## NOTE: Ignored if auth.token.type=simple
    ##
    ttl: 10m
  ## TLS authentication for client-to-server communications
  ## ref: https://etcd.io/docs/current/op-guide/security/
  ##
  client:
    ## @param auth.client.secureTransport Switch to encrypt client-to-server
    communications using TLS certificates
    ##
    secureTransport: true
    ## @param auth.client.useAutoTLS Switch to automatically create the TLS
    certificates
    ##
    useAutoTLS: false
    ## @param auth.client.existingSecret Name of the existing secret containing
    the TLS certificates for client-to-server communications
    ##
    existingSecret: ""
    ## @param auth.client.enableAuthentication Switch to enable host
    authentication using TLS certificates. Requires existing secret
    ##
    enableAuthentication: true
    ## @param auth.client.certFilename Name of the file containing the client
    certificate
    ##
    certFilename: cert.pem
    ## @param auth.client.certKeyFilename Name of the file containing the client
    certificate private key
    ##
    certKeyFilename: key.pem
    ## @param auth.client.caFilename Name of the file containing the client CA
    certificate
    ## If not specified and `auth.client.enableAuthentication=true` or
    `auth.rbac.enabled=true`, the default is is `ca.crt`
    ##
    caFilename: "ca.pem"
    ## @param auth.client.certDuration Requested duration the signed certificate
    will be valid for
    ##
    certDuration: ""

```

```

    ## @param auth.client.certExtraDnsSans DNS Subject Alternative Name to add to
the certificates
    ##
    certExtraDnsSans: ""
    ## @param auth.client.certExtraIpSans IP Subject Alternative Name to add to
the certificates
    ##
    certExtraIpSans: ""
    ## TLS authentication for server-to-server communications
    ## ref: https://etcd.io/docs/current/op-guide/security/
    ##
    peer:
        ## @param auth.peer.secureTransport Switch to encrypt server-to-server
communications using TLS certificates
        ##
        secureTransport: true
        ## @param auth.peer.useAutoTLS Switch to automatically create the TLS
certificates
        ##
        useAutoTLS: false
        ## @param auth.peer.existingSecret Name of the existing secret containing the
TLS certificates for server-to-server communications
        ##
        existingSecret: ""
        ## @param auth.peer.enableAuthentication Switch to enable host authentication
using TLS certificates. Requires existing secret
        ##
        enableAuthentication: true
        ## @param auth.peer.certFilename Name of the file containing the peer
certificate
        ##
        certFilename: cert.pem
        ## @param auth.peer.certKeyFilename Name of the file containing the peer
certificate private key
        ##
        certKeyFilename: key.pem
        ## @param auth.peer.caFilename Name of the file containing the peer CA
certificate
        ## If not specified and `auth.peer.enableAuthentication=true` or
`rbac.enabled=true`, the default is is `ca.crt`
        ##
        caFilename: "ca.pem"
        ## @param auth.peer.certDuration Requested duration the signed certificate
will be valid for
        ##
        certDuration: ""
        ## @param auth.peer.certExtraDnsSans DNS Subject Alternative Name to add to
the certificates
        ##
        certExtraDnsSans: ""
        ## @param auth.peer.certExtraIpSans IP Subject Alternative Name to add to the
certificates
        ##

```

```

    certExtraIpSans: ""
## @param autoCompactionMode Auto compaction mode, by default periodic. Valid
values: "periodic", "revision".
## - 'periodic' for duration based retention, defaulting to hours if no time unit
is provided (e.g. 5m).
## - 'revision' for revision number based retention.
##
autoCompactionMode: ""
## @param autoCompactionRetention Auto compaction retention for mvcc key value
store in hour, by default 0, means disabled
##
autoCompactionRetention: ""
## @param heartbeatInterval Cluster leader heartbeat interval, in ms (by default
100)
## Refer to https://etcd.io/docs/v3.5/tuning/#time-parameters
##
heartbeatInterval: ""
## @param electionTimeout Timeout after which a follower will start an election
when not receiving a leader heartbeat, in ms (by default 1000)
## Refer to https://etcd.io/docs/v3.5/tuning/#time-parameters
##
electionTimeout: ""
## @param clusterName Cluster name - this is the name of the etcd cluster.
##
clusterName: "sanetcd"
## @param existingEndpoints Existing cluster endpoints to use for bootstrapping.
## When this is set, the etcd instance created by this chart will add itself as a
member of the cluster.
## An example is: "https://etcd1:2379,https://etcd2:2379"
##
existingEndpoints: ""
## @param initialCluster Initial cluster configuration for bootstrapping.
## When existingEndpoints is specified, this parameter is ignored.
## If existingEndpoints and this parameter are not specified, etcd will default to
"default=http://localhost:2380"
## An example is: "etcd1=https://etcd1:2380,etcd2=https://
etcd2:2380,etcd3=https://etcd3:2380"
##
initialCluster: ""
## @param initialClusterState Initial cluster state. Allowed values: 'new' or
'existing'.
## If this values is not set, the default values below are set:
## - 'new': when installing the chart ('helm install ...')
## - 'existing': when upgrading the chart ('helm upgrade ...') or when
existingEndpoints is set
##
initialClusterState: ""
## @param discoverySrv DNS SRV domain used to bootstrap the cluster.
## ref: https://etcd.io/docs/v3.5/op-guide/clustering/#dns-discovery
##
discoverySrv: ""
## @param discoverySrvName Suffix to the DNS SRV name queried when bootstrapping
using DNS.

```

```

## ref: https://etcd.io/docs/v3.5/op-guide/clustering/#dns-discovery
##
discoverySrvName: ""
## @param memberCount Number of etcd member(s) to deploy. Maximum value: 3.
## WARNING: This parameter MUST NOT be modified during an upgrade. Modifying this
## value will cause the etcd member(s) to be restarted,
## potentially causing an unrecoverable loss of quorum.
##
memberCount: 1
## @param maxProcs Limits the number of operating system threads that can execute
## user-level
## Go code simultaneously by setting GOMAXPROCS environment variable
## ref: https://golang.org/pkg/runtime
##
maxProcs: ""
## @param removeMemberOnUninstall Use a pre-delete chart hook to remove the etcd
## member from the etcd cluster on chart uninstall
##
removeMemberOnUninstall: true
## @param configuration etcd configuration. Specify content for etcd.conf.yml
## e.g:
## configuration: |-
##     foo: bar
##     baz:
##
configuration: ""
## @param existingConfigmap Existing ConfigMap with etcd configuration
## NOTE: When it's set the configuration parameter is ignored
##
existingConfigmap: ""
## @param extraEnvVars [array] Extra environment variables to be set on etcd
## container
## e.g:
## extraEnvVars:
##   - name: FOO
##     value: "bar"
##
extraEnvVars: []
## @param extraEnvVarsCM Name of existing ConfigMap containing extra env vars
##
extraEnvVarsCM: ""
## @param extraEnvVarsSecret Name of existing Secret containing extra env vars
##
extraEnvVarsSecret: ""
## @param command [array] Default container command (useful when using custom
## images)
##
command: []
## @param args [array] Default container args (useful when using custom images)
##
args: []

## @section etcd statefulset parameters

```



```

statefulset:
  ## @param statefulset.enabled create statefulset if equal true
  ##
  enabled: true

## Update strategy
## ref: https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/
## update-strategies
## @param updateStrategy.type Update strategy type, can be set to RollingUpdate or
## OnDelete.
##
updateStrategy:
  type: RollingUpdate
## @param podManagementPolicy Pod management policy for the etcd statefulset
## ref: https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/
## pod-management-policies
##
podManagementPolicy: Parallel
## @param hostAliases [array] etcd pod host aliases
## ref: https://kubernetes.io/docs/concepts/services-networking/add-entries-to-
## pod-etc-hosts-with-host-aliases/
##
hostAliases: []
## @param lifecycleHooks [object] Override default etcd container hooks
##
lifecycleHooks: {}
## etcd container ports to open
## @param containerPorts.client Client port to expose at container level
## @param containerPorts.peer Peer port to expose at container level
##
containerPorts:
  client: 2379
  peer: 2380
## etcd pods' Security Context
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/security-context/
## set-the-security-context-for-a-pod
## @param podSecurityContext.enabled Enabled etcd pods' Security Context
## @param podSecurityContext.fsGroup Set etcd pod's Security Context fsGroup
##
podSecurityContext:
  enabled: true
  fsGroup: 1001
## etcd containers' SecurityContext
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/security-context/
## set-the-security-context-for-a-container
## @param containerSecurityContext.enabled Enabled etcd containers' Security
## Context
## @param containerSecurityContext.runAsUser Set etcd container's Security Context
## runAsUser
## @param containerSecurityContext.runAsNonRoot Set etcd container's Security
## Context runAsNonRoot
##

```

```

containerSecurityContext:
  enabled: true
  runAsUser: 1001
  runAsNonRoot: true
## etcd containers' resource requests and limits
## ref: https://kubernetes.io/docs/user-guide/compute-resources/
## We usually recommend not to specify default resources and to leave this as a
conscious
## choice for the user. This also increases chances charts run on environments
with little
## resources, such as Minikube. If you do want to specify resources, uncomment the
following
## lines, adjust them as necessary, and remove the curly braces after 'resources:'.
## @param resources.limits [object] The resources limits for the etcd container
## @param resources.requests [object] The requested resources for the etcd
container
##
resources:
  limits:
    cpu: 1
    memory: 2Gi
  requests:
    cpu: 1m
    memory: 128Mi
## Configure extra options for liveness probe
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-
liveness-readiness-startup-probes/#configure-probes
## @param livenessProbe.enabled Enable livenessProbe
## @param livenessProbe.initialDelaySeconds Initial delay seconds for
livenessProbe
## @param livenessProbe.periodSeconds Period seconds for livenessProbe
## @param livenessProbe.timeoutSeconds Timeout seconds for livenessProbe
## @param livenessProbe.failureThreshold Failure threshold for livenessProbe
## @param livenessProbe.successThreshold Success threshold for livenessProbe
##
livenessProbe:
  enabled: true
  initialDelaySeconds: 300
  periodSeconds: 30
  timeoutSeconds: 5
  successThreshold: 1
  failureThreshold: 5
## Configure extra options for readiness probe
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-
liveness-readiness-startup-probes/#configure-probes
## @param readinessProbe.enabled Enable readinessProbe
## @param readinessProbe.initialDelaySeconds Initial delay seconds for
readinessProbe
## @param readinessProbe.periodSeconds Period seconds for readinessProbe
## @param readinessProbe.timeoutSeconds Timeout seconds for readinessProbe
## @param readinessProbe.failureThreshold Failure threshold for readinessProbe
## @param readinessProbe.successThreshold Success threshold for readinessProbe
##

```

```

## BE CAREFUL!!! If using a Service, traffic will not be sent to the Pods until
they are Ready.
## This can lead to a deadlock where the etcd members cannot communicate and start
the cluster.
##
readinessProbe:
  enabled: false
  initialDelaySeconds: 10
  periodSeconds: 10
  timeoutSeconds: 5
  successThreshold: 1
  failureThreshold: 5
## Configure extra options for liveness probe
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-
liveness-readiness-startup-probes/#configure-probes
## @param startupProbe.enabled Enable startupProbe
## @param startupProbe.initialDelaySeconds Initial delay seconds for startupProbe
## @param startupProbe.periodSeconds Period seconds for startupProbe
## @param startupProbe.timeoutSeconds Timeout seconds for startupProbe
## @param startupProbe.failureThreshold Failure threshold for startupProbe
## @param startupProbe.successThreshold Success threshold for startupProbe
##
startupProbe:
  enabled: false
  initialDelaySeconds: 0
  periodSeconds: 10
  timeoutSeconds: 5
  successThreshold: 1
  failureThreshold: 60
## @param customLivenessProbe [object] Override default liveness probe
##
customLivenessProbe: {}
## @param customReadinessProbe [object] Override default readiness probe
##
customReadinessProbe: {}
## @param customStartupProbe [object] Override default startup probe
##
customStartupProbe: {}
## @param extraVolumes [array] Optionally specify extra list of additional volumes
for etcd pods
##
extraVolumes: []
## @param extraVolumeMounts [array] Optionally specify extra list of additional
volumeMounts for etcd container(s)
##
extraVolumeMounts: []
## @param initContainers [array] Add additional init containers to the etcd pods
## e.g:
## initContainers:
##   - name: your-image-name
##     image: your-image
##     imagePullPolicy: Always
##     ports:

```

```

##      - name: portname
##      containerPort: 1234
##
initContainers: []
## @param sidecars [array] Add additional sidecar containers to the etcd pods
## e.g:
## sidecars:
##   - name: your-image-name
##     image: your-image
##     imagePullPolicy: Always
##     ports:
##       - name: portname
##         containerPort: 1234
##
sidecars: []
## @param podAnnotations [object] Annotations for etcd pods
## ref: https://kubernetes.io/docs/concepts/overview/working-with-objects/
## annotations/
##
podAnnotations: {}
## @param podLabels [object] Extra labels for etcd pods
## Ref: https://kubernetes.io/docs/concepts/overview/working-with-objects/labels/
##
podLabels: {}
## @param podLabelsTemplate [object] Extra labels for etcd pods that can contain
## variables
##
podLabelsTemplate: {}
## @param affinity [object] Affinity for pod assignment
## Ref: https://kubernetes.io/docs/concepts/configuration/assign-pod-node/
## #affinity-and-anti-affinity
##
affinity: {}
## @param nodeSelector [object] Node labels for pod assignment
## Ref: https://kubernetes.io/docs/user-guide/node-selection/
##
nodeSelector: {}
## @param tolerations [array] Tolerations for pod assignment
## Ref: https://kubernetes.io/docs/concepts/configuration/taint-and-toleration/
##
tolerations: []
## @param terminationGracePeriodSeconds Seconds the pod needs to gracefully
## terminate
## ref: https://kubernetes.io/docs/concepts/containers/container-lifecycle-hooks/
## #hook-handler-execution
##
terminationGracePeriodSeconds: ""
## @param schedulerName Name of the k8s scheduler (other than default)
## ref: https://kubernetes.io/docs/tasks/administer-cluster/configure-multiple-
## schedulers/
##
schedulerName: ""
## @param priorityClassName Name of the priority class to be used by etcd pods

```

```

## Priority class needs to be created beforehand
## Ref: https://kubernetes.io/docs/concepts/configuration/pod-priority-preemption/
##
priorityClassName: ""
## @param topologySpreadConstraints Topology Spread Constraints for pod assignment
## https://kubernetes.io/docs/concepts/workloads/pods/pod-topology-spread-constraints/
## The value is evaluated as a template
##
topologySpreadConstraints: []

## @section Service exposing the etcd member outside the Kubernetes cluster

service:
  ## @param service.type Kubernetes Service type. Supported value: "NodePort" and "LoadBalancer"
  ## Note: There is always a headless service enabled to expose the etcd member within the Kubernetes cluster
  ##
  type: ""
  ## @param service.enabled create service to expose etcd outside a Kubernetes cluster in combination with sdrp-operator if equal true
  ##
  enabled: false
  ## @param service.dualStack exposes the service on both IPv4 and IPv6 if available when set to true
  ##
  dualStack: false
  ## @param service.clusterIP Kubernetes service Cluster IP
  ## e.g.:
  ## clusterIP: None
  ##
  clusterIP: ""
  ## @param service.ports.client etcd client port
  ## @param service.ports.peer etcd peer port
  ##
  ports:
    client: 2379
    peer: 2380
  ## @param service.nodePorts.client Specify the nodePort client value for the LoadBalancer and NodePort service types.
  ## @param service.nodePorts.peer Specify the nodePort peer value for the LoadBalancer and NodePort service types.
  ## ref: https://kubernetes.io/docs/concepts/services-networking/service/#type-nodeport
  ##
  nodePorts:
    client: ""
    peer: ""
  ## @param service.loadBalancerIP loadBalancerIP for the etcd service (optional, cloud specific)
  ## ref: https://kubernetes.io/docs/user-guide/services/#type-loadbalancer
  ##

```

```

loadBalancerIP: ""
## @param service.loadBalancerSourceRanges [array] Load Balancer source ranges
## ref: https://kubernetes.io/docs/tasks/access-application-cluster/configure-
cloud-provider-firewall/#restrict-access-for-loadbalancer-service
## e.g:
## loadBalancerSourceRanges:
##   - 10.10.10.0/24
##
loadBalancerSourceRanges: []
## @param service.externalIPs [array] External IPs
## ref: https://kubernetes.io/docs/concepts/services-networking/service/
#external-ips
##
externalIPs: []
## @param service.externalTrafficPolicy %%MAIN_CONTAINER_NAME%% service external
traffic policy
## ref http://kubernetes.io/docs/tasks/access-application-cluster/create-
external-load-balancer/#preserving-the-client-source-ip
##
externalTrafficPolicy: Cluster
## @param service.extraPorts Extra ports to expose (normally used with the
'sidecar' value)
##
extraPorts: []
## @param service.labels [object] Additional labels for the etcd service
##
labels: {}
## @param service.annotations [object] Additional annotations for the etcd
service
##
annotations: {}
## @param service.sessionAffinity Session Affinity for Kubernetes service, can
be "None" or "ClientIP"
## If "ClientIP", consecutive client requests will be directed to the same Pod
## ref: https://kubernetes.io/docs/concepts/services-networking/service/
#virtual-ips-and-service-proxies
##
sessionAffinity: None
## @param service.sessionAffinityConfig Additional settings for the
sessionAffinity
## sessionAffinityConfig:
##   clientIP:
##     timeoutSeconds: 300
##
sessionAffinityConfig: {}
## @param service.sdrpScope When using sdrp-operator, this is the scope where
the SRV record is published.
## The A/AAAA record will always be published in the cluster scope.
## Allowed value: "global" or "cluster"
## Depending on this value, also configure "sdrpClusterDomain" or
"sdrpGlobalDomain" to enable automation
## of the configuration of the peer urls of this member with the fqdn of this
service published by sdrp-operator.

```

```

##
sdrpScope: "global"
## @param service.sdrpClusterDomain Cluster domain where the service is
published when using sdrp-operator
## This allow generating a fqdn representing the service globally.
## Required to allow geo-distributed etcd cluster when using a service of type
"LoadBalancer".
##
sdrpClusterDomain: ""
## @param service.sdrpGlobalDomain Global domain where the service is published
when using sdrp-operator
## This allow generating a fqdn representing the service globally.
##
sdrpGlobalDomain: ""
## @param service.sdrpClientFqdnInstance Overrides the instance part of the FQDN
for the etcd client SRV record published for the service.
## When it is used: <k8s service name>._<type>._<protocol>.<domain> ->
<instance>._<type>._<protocol>.<domain>
## Fill this with the same in every Helm release when deploying multiple
instances of this chart (i.e. multicluster)
## to publish SRV records for all instances under the same FQDN
sdrpClientFqdnInstance: ""
## @param service.extraFqdns [array] Extra fqdn(s) representing this service
## When cert-manager is generating certificates, this fqdn(s) will be added in
the certificate SAN.
## This fqdn(s) will also be added to the etcd member advertised url(s). The
fqdn(s) MUST be resolvable,
## otherwise, the etcd member will be unusable.
## NOTE: When using a service of type "LoadBalancer" and not using the sdrp-
operator, this allow providing
## a fqdn representing the load balancer.
## NOTE: When using a service of type "NodePort", this allow providing node(s)
fqdn. You will need to manually
## update the etcd member to add the peer urls based on this fqdn(s) once a port
is assigned.
##
extraFqdns: []

## @section networkInterface
## Using pod network interface for etcd communications
## When using TLS it is mandatory to either provide static ip or configure sdrp
operator
## For using sdrp operator, the interface, sdrpScope and sdrpClusterDomain values
should be provided
## For using static ip, the ip value should be defined
##
networkInterface:
  ## @param networkInterface.name selected network interface information for etcd
communication
  ## Etcd will be exposed through the selected network interface
  ## It should be chosen according to the name defined in networkAnnotation in the
networkAnnotations section

```

```

## To enable using the network interface the name of available network should be
provided
##
name: 'ext-static-net-1'
## @param networkInterface.interface This is the name of interface that etcd
will be exposed through.
## This variable should be provided when using sdrp operator
##
interface: 'net1'
## @param networkInterface.ip The ip that etcd will be exposed through.
## This variable should be specified when using static ip deployment
##
ip: '10.52.154.136'
## @param networkInterface.disableIPv6Autoconfig If true, auto-config will be
disabled (only for ipv6)
## warning: enabling this parameter will force etcd chart to run sysctl command
in privileged mode.
## suggestion: disable ipv6 autoconfig by placing sysctl in a tuning cni plugin
section of the NetworkAttachmentDefinition.
##
disableIPv6Autoconfig: false
## @param networkInterface.mtu This is to apply the mtu to the network interface
##
mtu: ''
## @param networkInterface.addressIndex Index of IP address to use from attached
network
## For example, can be used for selecting an IPv6 address on a dual-stack
network
##
addressIndex: 0
## @param networkInterface.defaultRoute This is the optional variable that will
be provided to k8s.v1.cni.cncf.io/networks annotation of pod
## It will be assigned to the "default-route" of k8s.v1.cni.cncf.io/networks
annotation
##
defaultRoute: '10.52.154.1'
## @param networkInterface.namespace This is the optional variable that will be
provided to k8s.v1.cni.cncf.io/networks annotation of pod
## It will be assigned to the "namespace" of k8s.v1.cni.cncf.io/networks
annotation
##
namespace: ''
## @param networkInterface.sdrpScope When using sdrp-operator, this is the scope
where the SRV record is published.
## The A/AAAA record will always be published in the cluster scope.
## Allowed value: "global" or "cluster"
sdrpScope: ''
## @param networkInterface.sdrpClusterDomain domain where the network interface
is published when using sdrp-operator in the scope
## This allow generating a fqdn representing the network interface in the scope.
## this is the variable that shows to use the sdrp.
sdrpClusterDomain: ''

```



```

    ## @param service.sdrpClientFqdnInstance Overrides the instance part of the FQDN
    ## for the etcd client SRV record published for the service.
    ## When it is used: <k8s service name>._<type>._<protocol>.<domain> ->
    <instance>._<type>._<protocol>.<domain>
    ## Fill this with the same in every Helm release when deploying multiple
    ## instances of this chart (i.e. multicluster)
    ## to publish SRV records for all instances under the same FQDN
    sdrpClientFqdnInstance: ''

## @section Persistence parameters

## Enable persistence using Persistent Volume Claims
## ref: https://kubernetes.io/docs/user-guide/persistent-volumes/
##
persistence:
    ## @param persistence.enabled If true, use a Persistent Volume Claim. If false,
    ## use emptyDir.
    ##
    enabled: true
    ## @param persistence.storageClass Persistent Volume Storage Class
    ## If defined, storageClassName: <storageClass>
    ## If set to "-", storageClassName: "", which disables dynamic provisioning
    ## If undefined (the default) or set to null, no storageClassName spec is
    ## set, choosing the default provisioner. (gp2 on AWS, standard on
    ## GKE, AWS & OpenStack)
    ##
    storageClass: ""
    ##
    ## @param persistence.annotations [object] Annotations for the PVC
    ##
    annotations: {}
    ## @param persistence.accessModes Persistent Volume Access Modes
    ##
    accessModes:
        - ReadWriteOnce
    ## @param persistence.size PVC Storage Request for etcd data volume
    ##
    size: 1Gi
    ## @param persistence.selector [object] Selector to match an existing Persistent
    ## Volume
    ## ref: https://kubernetes.io/docs/concepts/storage/persistent-volumes/#selector
    ##
    selector: {}

## @section Volume Permissions parameters

## Init containers parameters:
## volumePermissions: Change the owner and group of the persistent volume
## mountpoint to runAsUser:fsGroup values from the securityContext section.
##
volumePermissions:
    ## @param volumePermissions.enabled Enable init container that changes the owner
    ## and group of the persistent volume(s) mountpoint to `runAsUser:fsGroup`

```

```

##
enabled: false
## @param volumePermissions.image.repository Init container volume-permissions
image name
## @param volumePermissions.image.tag Init container volume-permissions image
tag
## @param volumePermissions.image.pullPolicy Init container volume-permissions
image pull policy
##
image:
  repository: bitnami/os-shell
  tag: 12-debian-12-r21
  pullPolicy: IfNotPresent
## Init container' resource requests and limits
## ref: https://kubernetes.io/docs/user-guide/compute-resources/
## We usually recommend not to specify default resources and to leave this as a
conscious
## choice for the user. This also increases chances charts run on environments
with little
## resources, such as Minikube. If you do want to specify resources, uncomment
the following
## lines, adjust them as necessary, and remove the curly braces after
'resources:'.
## @param volumePermissions.resources.limits [object] Init container volume-
permissions resource limits
## @param volumePermissions.resources.requests [object] Init container volume-
permissions resource requests
##
resources:
  ## Example:
  ## limits:
  ##   cpu: 500m
  ##   memory: 1Gi
  limits: {}
  requests: {}

## @section Network Policy parameters
## ref: https://kubernetes.io/docs/concepts/services-networking/network-policies/
##
networkPolicy:
  ## @param networkPolicy.enabled Enable creation of NetworkPolicy resources
  ##
  enabled: false
  ## @param networkPolicy.allowExternal Don't require client label for connections
  ## When set to false, only pods with the correct client label will have network
  access to the ports
  ## etcd is listening on. When true, etcd will accept connections from any source
  ## (with the correct destination port).
  ##
  allowExternal: true
  ## @param networkPolicy.extraIngress [array] Add extra ingress rules to the
  NetworkPolicy
  ## e.g:

```

```

## extraIngress:
##   - ports:
##     - port: 1234
##     from:
##       - podSelector:
##         - matchLabels:
##           - role: frontend
##       - podSelector:
##         - matchExpressions:
##           - key: role
##             operator: In
##             values:
##               - frontend
##
extraIngress: []
## @param networkPolicy.extraEgress [array] Add extra ingress rules to the
NetworkPolicy
## e.g:
## extraEgress:
##   - ports:
##     - port: 1234
##     to:
##       - podSelector:
##         - matchLabels:
##           - role: frontend
##       - podSelector:
##         - matchExpressions:
##           - key: role
##             operator: In
##             values:
##               - frontend
##
extraEgress: []
## @param networkPolicy.ingressNSMatchLabels [object] Labels to match to allow
traffic from other namespaces
## @param networkPolicy.ingressNSPodMatchLabels [object] Pod labels to match to
allow traffic from other namespaces
##
ingressNSMatchLabels: {}
ingressNSPodMatchLabels: {}

## @section Snapshotting parameters

## Start a new etcd cluster recovering the data from an existing snapshot before
bootstrapping
##
startFromSnapshot:
## @param startFromSnapshot.enabled Initialize new cluster recovering an
existing snapshot
##
enabled: false
## @param startFromSnapshot.existingClaim Existing PVC containing the etcd
snapshot

```

```

##
existingClaim: ""
## @param startFromSnapshot.snapshotFilename Snapshot filename
##
snapshotFilename: ""
## Enable auto disaster recovery by periodically snapshotting the keyspace:
## - It creates a cronjob to periodically snapshotting the keyspace
## - It also creates a ReadWriteMany PVC to store the snapshots
##
disasterRecovery:
  ## @param disasterRecovery.enabled Enable auto disaster recovery by periodically
  snapshotting the keyspace
  ##
  enabled: false
  cronjob:
    ## @param disasterRecovery.cronjob.schedule Schedule in Cron format to save
    snapshots
    ## See https://en.wikipedia.org/wiki/Cron
    ##
    schedule: "*/30 * * * *"
    ## @param disasterRecovery.cronjob.historyLimit Number of successful finished
    jobs to retain
    ##
    historyLimit: 1
    ## @param disasterRecovery.cronjob.snapshotHistoryLimit Number of etcd
    snapshots to retain, tagged by date
    ##
    snapshotHistoryLimit: 1
    ## @param disasterRecovery.cronjob.podAnnotations [object] Pod annotations for
    cronjob pods
    ## ref: https://kubernetes.io/docs/concepts/overview/working-with-objects/
    annotations/
    ##
    podAnnotations: {}
    ## Configure resource requests and limits for snapshotter containers
    ## ref: https://kubernetes.io/docs/user-guide/compute-resources/
    ## We usually recommend not to specify default resources and to leave this as
    a conscious
    ## choice for the user. This also increases chances charts run on environments
    with little
    ## resources, such as Minikube. If you do want to specify resources, uncomment
    the following
    ## lines, adjust them as necessary, and remove the curly braces after
    'resources:'.
    ## @param disasterRecovery.cronjob.resources.limits [object] Cronjob container
    resource limits
    ## @param disasterRecovery.cronjob.resources.requests [object] Cronjob
    container resource requests
    ##
    resources:
      limits:
        cpu: 500m
        memory: 1Gi

```

```

    requests:
      cpu: 1m
      memory: 64Mi
    ## @param disasterRecovery.cronjob.nodeSelector Node labels for cronjob pods
assignment
    ## Ref: https://kubernetes.io/docs/user-guide/node-selection/
    ##
    nodeSelector: {}
    ## @param disasterRecovery.cronjob.tolerations Tolerations for cronjob pods
assignment
    ## Ref: https://kubernetes.io/docs/concepts/configuration/taint-and-toleration/
    ##
    tolerations: []

  pvc:
    ## @param disasterRecovery.pvc.existingClaim A manually managed Persistent
Volume and Claim
    ## If defined, PVC must be created manually before volume will be bound
    ## The value is evaluated as a template, so, for example, the name can depend
on .Release or .Chart
    ##
    existingClaim: ""
    ## @param disasterRecovery.pvc.size PVC Storage Request
    ##
    size: 1Gi
    ## @param disasterRecovery.pvc.storageClassName Storage Class for snapshots
volume
    ##
    storageClassName: managed-nfs-storage

## @section Service account parameters

serviceAccount:
  ## @param serviceAccount.create Enable/disable service account creation
  ##
  create: false
  ## @param serviceAccount.name Name of the service account to create or use
  ##
  name: ""
  ## @param serviceAccount.automountServiceAccountToken Enable/disable auto
mounting of service account token
  ## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-
service-account/#use-the-default-service-account-to-access-the-api-server
  ##
  automountServiceAccountToken: true
  ## @param serviceAccount.annotations [object] Additional annotations to be
included on the service account
  ##
  annotations: {}
  ## @param serviceAccount.labels [object] Additional labels to be included on the
service account
  ##

```

```

labels: {}

## @section Other parameters

## etcd Pod Disruption Budget configuration
## ref: https://kubernetes.io/docs/tasks/run-application/configure-pdb/
##
pdb:
  ## @param pdb.create Enable/disable a Pod Disruption Budget creation
  ##
  create: false
  ## @param pdb.minAvailable Minimum number/percentage of pods that should remain
  scheduled
  ##
  minAvailable: 1
  ## @param pdb.maxUnavailable Maximum number/percentage of pods that may be made
  unavailable
  ##
  maxUnavailable: ""

## @section Security parameters for service mesh
##
security:
  ## @param security.create Enable/disable service mesh security creation
  ##
  create: false
  ## @param security.allowPlaintextClient Switch to disable plaintext client. When
  false, client must have tls enabled
  ##
  allowPlaintextClient: false
  ## @param security.allowedClientNamespaces [array] List of namespaces that can
  use a client to talk to the etcd cluster
  ##
  allowedClientNamespaces: []
  ## @param security.allowedMemberNamespaces [array] List of namespaces that can
  have an etcd member in the cluster
  ##
  allowedMemberNamespaces: []

## @section Routing parameters for service mesh
##
routing:
  ## @param routing.create Enable/disable service mesh gateway creation for etcd
  ##
  create: false
  ## @param routing.enabled Enable/disable service mesh virtual service routing
  creation for etcd
  ##
  enabled: false
  ## ingress gateway ports to use for etcd
  ## @param routing.ingressGatewayPorts.client Client port to use at gateway level
  ## @param routing.ingressGatewayPorts.peer Peer port to use at gateway level
  ##

```

```

ingressGatewayPorts:
  client: 2379
  peer: 2380
  ## @param routing.allowedIpBlocks [array] List of single IP or CIDR that can use
  a client to talk to the etcd cluster or have an etcd member in the cluster
  ##
  allowedIpBlocks: []

## @section Prometheus Rule
##
prometheusRule:
  ## @param prometheusRule.create Specifies whether a PrometheusRule resource
  should be created (alerting rule definitions)
  ##
  # create: false
  ## @param prometheusRule.labels Specify additional labels so the Prometheus
  instance can discover the rules
  ##
  labels: {}

## @section Observability agent
##
obs:
  ## @param obs.enabled Enable/disable observability agent
  ##
  enabled: true
  ## @param obs.image image parameters
  ##
  image:
    ## @param obs.image.repository observability agent image name
    ##
    repository: ""
    ## @param obs.image.tag observability agent image tag
    ##
    tag: ""
    ## @param obs.image.pullPolicy observability agent image pull policy. Defaults
    to 'Always' if image tag is 'latest', else set to 'IfNotPresent'
    ##
    pullPolicy: IfNotPresent
    ## @param obs.podAnnotations [object] Annotations to add to the pod for
    observability (used for prometheus scraping)
    ##
    podAnnotations: {}
    ## @param obs.podLabelsTemplate [object] Labels to add to the pod for
    observability (used for pod monitoring) - can contain variables
    ##
    podLabelsTemplate: {}
    ## @param obs.logs log management settings
    ##
    logs:
      ## @param obs.logs.telemetry log telemetry config
      telemetry:

```

```

    ## @param obs.logs.telemetry.topic telemetry logs will be sent to this Kafka
topic
  topic: rbbn-otel-agent
  ## @param obs.logs.backendServers log backends
  ##
  backendServers: {}
    ## @param obs.logs.backendServers.elasticsearch elasticsearch backend
    ## Warning: username and password represent the name of the ENV variable
name
  ## that contains the username and password from the secret
  # elasticsearch:
  #   - endpoint: <elasticsearch server address>:443
  #   auth: True
  #   username: ELASTICSEARCH_USER
  #   password: ELASTICSEARCH_PASSWD
  #   index: <filebeat index>
  ## @param obs.logs.backendServers.kafka kafka backend
  ##
  # kafka:
  #   - endpoint: <kafka server address>:<kafka port>
  #   sslCert: KAFKA_CERT
  #   sslKey: KAFKA_KEY
  #   sslCa: KAFKA_CA
  ## @param obs.logs.elasticsearchSecretName Name of secret containing
elasticsearch environment variables
  ##
  elasticsearchSecretName: ""
  ## @param obs.logs.kafkaSecretName Name of secret containing elasticsearch
environment variables
  ##
  kafkaSecretName: ""

  ## @param obs.log.elasticsearchCreds elasticsearch credentials to create
  ##
  elasticsearchCreds:
    create: False
  ## @param obs.log.kafkaCreds kafka credentials to create
  ##
  kafkaCreds:
    create: False

## @section Common util
##
common-util:
  ## @param common-util.role Role for getting pod logs
  ##
  role:
    ## @param common-util.role.create Specifies whether a Role and RoleBinding
should be created for the observability components
    create: false
  ## @param global.obs.serviceAccount SA for observability
  ##
  serviceAccount:

```



```

    ## @param common-util.serviceAccount.create Specifies whether a service
account should be created for the observability components
    ##
    create: false
    ## @param common-util.serviceAccount.annotations Annotations to add to the
service account
    ##
    annotations: {}
    ## @param common-util.serviceAccount.name The name of the service account to
use.
    ## If not set and create is true, a name is generated using the fullname
template
    ##
    name: default
    ## @param common-util.logPersistentVolumeStorage Storage request limit for PVC
    ##
    logPersistentVolumeStorage:
    ## @param common-util.logPersistentVolumeStorage.create Specifies whether to
create a PVC for the storage of log entries
    ##
    create: true
    ## @param common-util.logPersistentVolumeStorage.storageClassName Specify the
storageClass to be used for the PVC.
    ##
    storageClassName: "managed-nfs-storage"
    persistence:
    ## @param common-util.persistence.annotations Annotations to add to the
PersistentVolumeClaims
    ##
    annotations:
    volume.beta.kubernetes.io/storage-provisioner: storage.io/nfs
    ## @param common-util.imageCredentials ImagePullSecret creation from credentials
    ##
    imageCredentials:
    ## @param common-util.imageCredentials.create Specifies whether an image
credentials secret should be created
    ##
    create: true
    ## @param common-util.imageCredentials.createPostDelete Specifies whether an
image credentials secret should be created as a post-delete hook
    ##
    createPostDelete: true
    ## @param common-util.prometheusRule Prometheus alerting rules
    ##
    prometheusRule:
    ## @param common-util.prometheusRule.create Specifies whether a PrometheusRule
resource should be created
    ##
    create: false

```

6. Repeat this procedure to set up all the three etcd instances on CNF.

For more information, refer to [RAMP CNF etcd Health Check](#).

etcd Parameters

You can customize the etcd installation using various parameters to suit your specific environment and requirements. Below are some commonly used parameters for installing etcd, typically specified in an etcd configuration file.

Parameters to Edit	Description	Example	Notes
imageCredentials	Credentials to artifactory.	<pre> global: imageCredentials: name: "" registry: "xxxxxx" username: "xxxxx" password: "xxxx" obs-common-modules: imageCredentials: # Specifies whether an image credentials secret should be created create: true ## @param imageRegistryPath Containers image repository path in the registry ## imageRegistryPath: "/" dockerhub-docker-remote" image: repository: bitnami/etcd tag: 3.5.7 ## Specify a imagePullPolicy ## Defaults to 'Always' if image tag is 'latest', else set to 'IfNotPresent' ## ref: https://kubernetes.io/ docs/user-guide/images/#pre- pulling-images ## pullPolicy: IfNotPresent </pre>	Leave the name field empty. Provide the registry from where the image is located. Under obs-common-modules, set create as "true" for "imageCredentials". Provide the imageRegistryPath and the pull policy.
cluster name	Provide a name for the etcd cluster.	<pre> clusterName: "etcdctl1" </pre>	

Parameters to Edit	Description	Example	Notes
existingEndpoints	current endpoints available in cluster (IP/FQDN)	IP: existingEndpoints: "http://172.29.208.33:30082/" FQDN : existingEndpoints: "http://worker-10.blr-cp1.lab.rbbn.com:30082/"	Parameter is not needed while creating the first etcd instance. It is only mandatory for the second and third etcd instances. Examples: "http://172.29.208.33:30082/", http://172.29.208.34:30083/".
initialCluster	Initial cluster configuration for bootstrap.	initialCluster: ""	If the existing endpoints are specified, this parameter is ignored.
initialClusterState	The initial state when a cluster is being created. Values are either 'new' or 'existing'.	initialClusterState="new"	If these values are not set, then set the following default values: 'new' - while installing the chart ('helm install ...') 'existing' - while upgrading the chart ('helm upgrade ') or while "existingEndpoints" are set.

Parameters to Edit	Description	Example	Notes
service	NodePort / clusterIP / LoadBalancer	NODEPORT : <pre> service: type: "NodePort" enabled: true ###ports in range 30000 - 32000 for host port nodePorts: client: "" peer: "" LoadBalancer : service: type: "LoadBalancer " enabled: true loadBalancerIP: "xx.xx.xx.xx" ## @param service.ports.client etcd client port ## @param service.ports.peer etcd peer port ## ports: client: 2379 peer: 2380 </pre>	By default, the ports are selected randomly. If you set the ports manually, then select the NodePort: - The host port range is 30000 - 32000 - When Loadbalancer is added as Service, the Service type is "Loadbalancer". - Provide the Loadbalancer IP address. - The default ports for loadbalancer are "2379" and "2380".

Parameters to Edit	Description	Example	Notes
networkInterface	Network Interface details for etcd. Ribbon recommends using multus or load balancer service for etcd.	<pre> networkInterface: name: 'ext-static-net-1' interface: 'net1' ip: '10.52.154.136' disableIPv6Autoconfig: false mtu: " addressIndex: 0 defaultRoute: '10.52.154.1' namespace: " sdrpScope : " sdrpClusterDomain: " sdrpClientFqdnInstance: " </pre>	• name: The name of interface that etcd will be exposed through. • interface: The name of the interface used for etcd. • ip: The ip that etcd will be exposed through. This variable should be specified when using static ip deployment. • disableIPv6Autoconfig: If true, auto-config will be disabled (only for ipv6). Enabling this parameter will force etcd chart to run sysctl command in privileged mode. Suggestion Disable ipv6 autoconfig by placing sysctl in a tuning cni plugin section of the NetworkAttachmentDefinition.

Parameters to Edit	Description	Example	Notes
			• mtu: This is to apply the mtu to the network interface. • addressIndex: Index of IP address to use from attached network For example, can be used for selecting an IPv6 address on a dual-stack network. • defaultRoute: This is the optional variable that will be provided to k8s.v1.cni.cncf.io/networks annotation of pod. It will be assigned to the "default-route" of k8s.v1.cni.cncf.io/networks annotation. • namespace: This is the optional variable that will be provided to k8s.v1.cni.cncf.io/networks annotation of pod. It will be assigned to the "namespace" of k8s.v1.cni.cncf.io/networks annotation. • sdrpScope: When using sdrp-operator, this is the scope where the SRV record is published. The A/AAAA record will always be published in the cluster scope. Allowed value: "global" or "cluster" sdrpScope: "

Parameters to Edit	Description	Example	Notes
			• sdrpClusterDomain: Domain where the network interface is published when using sdrp-operator in the scope. This allow generating a fqdn representing the network interface in the scope. This is the variable that shows to use the sdrp.' • sdrpClientFqdnInstance: Overrides the instance part of the FQDN for the etcd client SRV record published for the service. When it is used: <k8s service name>._<type>._<protocol>.<domain> -> <instance>._<type>._<protocol>.<domain> Fill this with the same in every Helm release when deploying multiple instances of this chart (i.e. multicluster) to publish SRV records for all instances under the same FQDN

Parameters to Edit	Description	Example	Notes
Certificates	1. CertManager 2. Client and Server certificates	<pre> certManager: enabled: true issuer: name: "<Name of Issuer>" kind: "<Issuer kind>" auth: client: secureTransport: true enableAuthentication: true certDuration: "" server: secureTransport: true enableAuthentication: true certDuration: "" </pre>	• Enable CertManager. • Provide the Issuer type and name. • If you are using NodePort with TLS, set the certExtraDnsSans parameters with the worker node name. • In values.yaml under auth, enable secureTransport and enableAuthentication as true • You can also provide the duration of expiry of certificate. The Client section provides information on the tls communication between endpoint, etcd, and server section among the etcds in a cluster. The client and server certificates use the port "2379". The client certificate is used for etcdctl.
volume obs	logPersistentVolumeStorage	<pre> # Storage request limit for PVC logPersistentVolumeStorage: # Specifies whether a # service account should be # created for the observability # components create: true </pre>	Enable logPersistentVolumeStorage for creating pvc for etcd.

Parameters to Edit	Description	Example	Notes
Role	Roles for SA.	<pre>roles: ## @param roles.create Enable/disable Role and RoleBinding creation. If set to false, the ServiceAccount passed in global will need the following rules: ## If using a NodePort service: ## - apiGroups: [""] # "" indicates the core API group ## resources: ["services"] ## verbs: ["get"] ## If using persistence: ## - apiGroups: [""] ## resources: ["persistentvolumeclaims"] ## verbs: ["get", "list", "delete", "deletecollection"] ## create: true</pre>	

Parameters to Edit	Description	Example	Notes
common-util	common-util details for etcd pod	<pre> common-util: role: create: false serviceAccount: create: false annotations: {} name: default logPersistentVolumeStorage: create: true storageClassName: "managed-nfs-storage" persistence: annotations: volume.beta.kubernetes.io/ storage-provisioner: storage.io/ nfs imageCredentials: create: true createPostDelete: true prometheusRule: create: false </pre>	• common-util.role.create: Specifies whether a Role and RoleBinding should be created for the observability components.

Parameters to Edit	Description	Example	Notes
			• common-util.serviceAccount.create: Specifies whether a service account should be created for the observability components. • common-util.serviceAccount.annotations: Annotations to add to the service account. • common-util.serviceAccount.name: The name of the service account to use. If not set and create is true, a name is generated using the fullname template. • common-util.logPersistentVolumeStorage.create: Specifies whether to create a PVC for the storage of log entries. • common-util.logPersistentVolumeStorage.storageClassName: Specify the storageClass to be used for the PVC. • common-util.persistence.annotations: Annotations to add to the PersistentVolumeClaims • common-util.imageCredentials ImagePullSecret: ImagePullSecret creation from credentials. • common-util.imageCredentials.create: Specifies whether an image credentials secret should be created. • common-util.imageCredentials.createPostDelete : Specifies whether an image credentials secret should be created as a post-delete hook.

Parameters to Edit	Description	Example	Notes
			common-util.prometheusRule.create: Specifies whether a PrometheusRule resource should be created.

Installing etcd on KVM

Create the etcd VMs on a KVM Platform

Perform the following steps to instantiate the etcd VMs on a KVM platform.

Prerequisite

- Three free IPs are required to allocate to the etcd instances.
- The recommended configuration is one vCPU, 2 GB of memory, and a minimum of 50 GB of disk space. For more information, refer to [RAMP etcd System Requirements](#).
- Verify the network interfaces are connected and operable.
- Verify whether you have obtained the necessary installation files:
 - ISO configuration files
 - qcow2 files
 For more information on using the portal, refer to [Download Files from Ribbon Support Portal](#).
- Create a customized ISO configuration drive for KVM. Refer to [Create an ISO Configuration Drive for VMware or KVM](#)

Start

1. Install the VNF using `virt-install`.

In the following example command:

`--network` assumes that a bridge called `br0` is the VNF's network interface. If you choose to deploy with two network interfaces, add another `--network` statement with the bridge for the second interface. The order of `--network` is the same as the order of interfaces in the VM (eth0).

Example

```
export VNF_NAME=ammanetcd # Replace with your desired VM name

sudo virt-install \
  --name $VNF_NAME \
  --memory 2048 \
  --disk /var/lib/libvirt/images/AppServices-22.07.00R000-B3500_vmCCS-1.4.1-B2297-x86_64.qcow2,device=disk,bus=virtio \
  --disk /var/lib/libvirt/images/etcd.iso,device=disk,bus=virtio,readonly=on \
```

```
--os-type linux \
--os-variant rhel8.2 \
--graphics none \
--network bridge=br0,model=virtio \
--import
```

2. Check the status of the VM instance using the following command:

```
virsh list
```

The following is an example output:

Example

Id	Name	State
1	ammanetcd	running

Note

Validate the VM name and ensure that the VM state appears as "running".

3. To validate that services are running once the VM is ready, check the status of `appservices` using the following command as `sysadm` user.

```
$ vmccs-status
```

Example vmccs-status output

```
$ vmccs-status
Validating backup-manager services status...
  backup-manager: active (running)
backup-manager is active

Validating Etcd services status...
  etcd: active (running)
Etcd is active

Validating Fluentbit services status...
  td-agent-bit: active (running)
  fluent-sd: active (running)
  fluent-sd-watch: active (running)
Fluentbit is active
```

```

Validating nginx services status...
  nginx: active (running)
  nginx-exporter: active (running)
nginx is active

Validating Node Exporter services status...
  node-exporter: active (running)
Node Exporter is active

Validating Prometheus services status...
  prometheus: active (running)
  prometheus-autoconfig: active (running)
  alertmanager: active (running)
  alertmanager-watch: active (running)
Prometheus is active

Validating SDR services status...
  sdr: active (running)
SDR is active

Validating VNF Operations services status...
  vnf-operations: active (running)
VNF Operations is active

All required vmCCS services are active.

```

Network **interface** roles

Default Gateway	Management	Internal	Signaling
eth0	eth0	eth0	eth0

To check the status of etcd cluster synchronization and health of any node, refer to [Health Check etcd](#).

Create an ISO Configuration Drive for VMware or KVM

Complete the following procedure to set up an ISO configuration drive.

Start

1. Log on to the Ribbon Support portal. Download the `AppServices-configDrive.img` files. For more information on using the portal, refer to [Download Files from Ribbon Support Portal](#).
2. Log on to a Linux server as the `root` user. On this server, create an `.iso` file from the provided template file (`AppServices-configDrive.img`) to use as a configuration drive for the VMs.

3. Create a temporary directory. In the following example the directory name is "etcd":

```
mkdir -p /tmp/etcd
```

4. Mount the image.

```
sudo mount AppServices-configDrive.img /tmp/etcd
```

5. Issue the following command to edit the cloud configuration. Refer to the following table for information on the parameters.

```
vim /tmp/etcd/user-data
```

Cloud Configuration Parameters

Parameters To Edit	Description	Example	Note
hostname	Hostname of the VM in use	hostname: "amma netcd"	
fqdn	FQDN of the VM in use	fqdn: "ammanetc d.local"	
timezone	Choose the time zone	timezone: "Asia/ Kolkata"	
ntp	NTP server IP	servers: ["10.128.254.67"]	

Parameters To Edit	Description	Example	Note
VnfName GatewayIpv4/ GatewayIpv6 Externallp	hostname: ammanetcd1 VnfName: amman- ramp-geo-cluster Gateway IP address of the etcd instance Externally visible IP address of the ETCD instance.	# Ribbon vmCCS userdata: - content: { "VnfName": "amman-ramp-geo- cluster",	◦ Net{1,2,3}: Definition for the interface IF{1,2,3} ◦ Enabled: Indicates if the interface is enabled. Enabled is mandatory. You must set it to "true" or "false". ◦ GatewayIpv4: IPv4 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface ◦ GatewayIpv6: IPv6 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface ◦ ExternalIp: External IP address for this interface ◦ Categories: List of category of traffic on this interface. By default, management is on net1, signaling and internal are on net2, and nothing is configured for net3. ◦ IsDefault: Indicates whether or not to assign the default route to this interface. Only one interface may have IsDefault=true. If false for all interfaces, the first interface with a gateway configured is assigned the default route. This parameter is not required if only one gateway was specified in the network-config file.

Parameters To Edit	Description	Example	Note
		<pre> "Networks": { "Net1": { "Enabled": "True", "GatewayIpv4": "", "GatewayIpv6": "fd00:10:6b50:40c0: :1", "Externallp": "fd00:10:6b50:40c0: :24", "Categories": [], "IsDefault": "True" }, "Net2": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "Externallp": "", "Categories": [], "IsDefault": "" }, "Net3": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "Externallp": "", "Categories": [], "IsDefault": "" } } </pre>	

Parameters To Edit	Description	Example	Note
Etcd	Etcd configuration	<pre> "Etcd": { "ExistingEndpoints" : [], "PersistentDataPath" : "", "PersistentBackupPath" : "", "RootPassword" : "", "UserName" : "", "UserPassword" : "", "ClientCert" : "", "ClientKey" : "", "ClientCaCert" : "", "ServerCert" : "", "ServerKey" : "", "ServerCaCert" : "", "PeerCert" : "", "PeerKey" : "", "PeerCaCert" : "", "HeartbeatInterval" : "", "ElectionTimeout" : "", "BackupDiskMaxUse" : "", "BackupDiskKeepFree" : "" </pre>	◦ PersistentDataPath: Path to the persistent disk to use for Etcd data. The virtio number corresponds to the Etcd data volume ID provided in the deployment. ◦ RootPassword: The Etcd database password for the root user. If left blank, no authentication is enabled on the database. In a HA setup, the passwords must match on all the virtual machines. ◦ UserName: The name of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank. ◦ UserPassword: The password of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank. ◦ HeartbeatInterval: The interval (in ms) at which the leader notifies followers that it is still the leader. The recommended value to set is around the maximum of average round-trip time (RTT) between members, it is normally around 0.5-1.5x the round-trip time. If this field is left blank or omitted, the default value is 100 ms.

Parameters To Edit	Description	Example	Note
		<pre>"BackupStartTime" : "", "BackupFullPeriod" : "0", "BackupRetention" : "" },</pre>	◦ ElectionTimeout: The duration (in ms) that a follower node performs without hearing a heartbeat before attempting to become the leader. The recommended value to set must be at least 10 times the RTT to account for a variance in the network. If this field is left blank or omitted, the default value is 1000 ms. ◦ BackupDiskMaxUse: The maximum percentage of the disk that allowed to be occupied by the Etcd backup files. The default value is 15. ◦ BackupDiskKeepFree: The percentage of disk that must be left free on the file system. The oldest backup files are deleted when this limit is reached. The default value is 30. ◦ BackupStartTime: The time of day when the scheduled backup starts. The format is in hh:mm±hh:mm. The first part of the format is the start time and second part is an offset (from UTC) to specify the time zone. If the time zone is not specified, then the local time zone of the virtual machine processing the request is used as the default time zone. The default value is 02:00.

Parameters To Edit	Description	Example	Note
			◦ BackupFullPeriod : The interval at which a full backup of the Etcd full is performed. This is expressed in the format of weeks and/or days, or hours. For example, 1w2d or 4h. Hours are not allowed to be provided with days or weeks. • The maximum allowed value for hours is 23h. • The minimum allowed value is 1h. • 0 means that no backup is performed. The default value is 1d. Note Set the BackupFullPeriod as 0 (Zero). ◦ BackupRetention : Specifies how long the backup files are retained before deleting the file(s). An empty value means that the backup files are retained for 7 days. This is expressed in the format of weeks, days and/or hours. For example, 1w24h or 2d.

Parameters To Edit	Description	Example	Note
EtcdRegistries	Information to connect to the ETCD cluster	<pre>"VnfOperations": { "EtcdRegistries": [], "EtcdUserName": "admin", "EtcdUserPassword": "admin", "Salt": "mysalt@123"</pre>	VM communicate uses this function with the ETCD cluster for network function coordination, for example to register this VM for monitoring. Information on how to reach the ETCD cluster members and the options on how to fill this field are explained below: ◦ Recommended: Single entry pointing to an SRV FQDN that then points to all ETCD instances. This is recommended because SRV records can be updated with topology changes. ◦ Empty: This will cause the VM to always communicate to the local ETCD which has knowledge of the List of all planned members IPs.
VnfExistingInstances	IP addresses of any etcd instances created before	<pre>"VnfExistingInstances": ["10.54.8.166","10.54.8.165"], "VnfReplaceInstance" : "", "UseMongoDB" : "", "UseEtcd" : "True", "UsePrometheus" : "True", "UseAlertManager" : "True",</pre>	While creating the first instance, "VnfExistingInstances" does not contain any value. While creating the second instance, "VnfExistingInstances" must contain the IP address of first etcd instance that was created. While creating the third instance, "VnfExistingInstances" must contain the IP addresses of the first and second etcd instances that were created.

Parameters To Edit	Description	Example	Note
Prometheus	Prometheus configuration	"Prometheus": { "PersistentDataPath" : "", "MaxDiskUsage" : "40" }	Prometheus configuration Fields: ◦ PersistentDataPath: Path to the persistent disk to use for Prometheus and AlertManager data. The virtio number corresponds to the Prometheus data volume ID provided in the deployment. ◦ MaxDiskUsage: Maximum disk usage allowed by Prometheus data in percent of the total disk size.

Sample etcd Userdata

```
#cloud-config

# Hostname to use for this VM
hostname: "ammanetcd"

# FQDN to use for this VM, usually just <hostname>.local
fqdn: "ammanetcd.local"

# DO NOT CHANGE
preserve_hostname: false

# DO NOT CHANGE
manage_etc_hosts: true

# List of groups to create on this VM
groups:
  # User part of this group can read backup files
  - backup_group # This group name is used by ansible during the VM initial
    configuration

# List of users to create/update on this VM
users:
  # Recommended user for systems administrators
  - name: root
    plain_text_passwd: "Sonus@123"
    lock_passwd: false

  - name: sysadm
    plain_text_passwd: "shipped!!"
    lock_passwd: false
```

```

    ssh_authorized_keys:
      - "ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAQEAqJX+iihNxOPZNHwBXbEogknmUH2xvupn8/
bcx9YmAT7RcVsJ4ICMIGic1yAJjhdRWgTRwpGqBKzftUVanBZS232aBETPMGZHgTdpjpFdUMGHiYU4niwmmw
Gzp84mnyZoqwh5pGau9ZTJL2IUjyh0t7a/s2RXHu88HHC4+SduD5fWiU0GL0bc8re2lXdkUIlk/
Sg430GNqHW68SnZI7yPWZJbv9z3+6qN2oxvBqd/
eb9RbQQzoupSci0BFBkYhUiRFbNQZAcTF7+4XFkraSnBLtYckN+EPDJv4G/
Uk9bi65320g5SQPFoXEzenk2STLJq0tiCcMeX04fIw0bhC0SgQ== ssequeira@ptbats"

# Timezone for this VM (format: tz database, e.g. "America/New_York")
timezone: "Asia/Kolkata"

# List of NTP servers to use on this VM
ntp:
  servers: ["10.128.254.67"]
  ntp_client: chrony # DO NOT CHANGE
  config:
    service_name: chronyd # DO NOT CHANGE

# Files that will be written to disk
write_files:
  # DO NOT CHANGE
  - content: |
      {
        "TemplateName": "heat_template.yaml"
      }
    path: /opt/rbbn/userData.json
    owner: root:root
    permissions: '0600'

# Ribbon vmCCS userdata: fill in all fields according to user guide
- content: |
    {
      "VnfName": "amman-ramp-geo-cluster",

      "Networks": {
        "Net1": {
          "Enabled": "True",
          "GatewayIpv4": "",
          "GatewayIpv6": "",
          "ExternalIp": "172.19.52.209",
          "Categories": [],
          "IsDefault": "true"
        },
        "Net2": {
          "Enabled": "False",
          "GatewayIpv4": "",
          "GatewayIpv6": "",
          "ExternalIp": "",
          "Categories": [],
          "IsDefault": "false"
        }
      },
    },

```

```
"Net3": {
  "Enabled": "False",
  "GatewayIpv4": "",
  "GatewayIpv6": "",
  "ExternalIp": "",
  "Categories": [],
  "IsDefault": "false"
}
},

"VnfOperations": {
  "EtcdRegistries": [],
  "EtcdUserName": "",
  "EtcdUserPassword": "",
  "Salt": ""
},

"ServiceDiscovery": {
  "RegistryType": "dns",
  "Registries": []
},

"Logging": {
  "Elasticsearch": {
    "Hosts": [{
      "Addr": "",
      "Port": "",
      "HttpUser": "",
      "HttpPasswd": "",
      "TlsEnable": "Off",
      "TlsVerify": "On",
      "RecordTypeFilters": ["tdr","log"]
    }],
    "Index": ""
  },
  "Syslog": {
    "Hosts": [{
      "Addr": "10.54.21.201",
      "Port": "514",
      "RecordTypeFilters": ["tdr","log"]
    }],
    "Protocol": "udp",
    "CACert": ""
  },
  "Fluent": {
    "Hosts": [{
      "Addr": "",
      "Port": "",
      "RecordTypeFilters": ["tdr","log"]
    }]
  }
},
},
```



```

    "Metrics": {
        "Export": "True"
    }
}
path: /etc/rbbn/podman/userdata.json
owner: root:root
permissions: '0600'

# Ribbon AppServices userdata: fill in all fields according to user guide
- content: |
{
  "VnfExistingInstances" : ["172.19.52.139","172.19.52.129"],
  "VnfReplaceInstance"   : "",
  "UseMongoDB"           : "False",
  "UseEtcd"              : "True",
  "UsePrometheus"        : "True",
  "UseAlertManager"      : "True",

  "MongoDB": {
    "PersistentDataPath"      : "",
    "PersistentBackupPath"    : "",
    "AuthKey"                 : "",
    "AdminPassword"          : "",
    "UserName"                : "",
    "UserPassword"           : "",
    "BackupDiskMaxUse"        : "15",
    "BackupDiskKeepFree"     : "30",
    "BackupStartTime"         : "02:00",
    "BackupFullPeriod"        : "1d",
    "BackupDifferentialPeriod" : "4h",
    "BackupRetention"         : ""
  },

  "Etcd": {
    "ExistingEndpoints" : [],
    "PersistentDataPath" : "",
    "PersistentBackupPath" : "",
    "RootPassword"       : "",
    "UserName"           : "",
    "UserPassword"       : "",
    "ClientCert"         : "",
    "ClientKey"          : "",
    "ClientCaCert"       : "",
    "ServerCert"         : "",
    "ServerKey"          : "",
    "ServerCaCert"       : "",
    "PeerCert"           : "",
    "PeerKey"            : "",
    "PeerCaCert"         : "",
    "HeartbeatInterval"  : "100",
    "ElectionTimeout"     : "1000",
    "BackupDiskMaxUse"    : "15",
    "BackupDiskKeepFree" : "30",

```

```

        "BackupStartTime"      : "02:00",
        "BackupFullPeriod"    : "0",
        "BackupRetention"     : ""
    },

    "Prometheus": {
        "PersistentDataPath"   : "",
        "MaxDiskUsage"         : "40"
    }
}
path: /etc/rbbn/appservices/userdata.json
owner: root:root
permissions: '0600'

# DO NOT CHANGE
runcmd:
    # Launch main vmCCS playbook (downstream plays are launched by this playbook)
    - ansible-playbook /etc/rbbn/podman/configure.yml

```

6. Issue the following command to edit the network configuration:

```
vim /tmp/etcd/network-config
```

Edit the following parameters in the network-config file:

Parameters to edit	Description	Example
addresses	IP address to assign to this interface.	# DO NOT CHANGE version: 2
gateway4/gateway6	The default IP gateway.	# List of network interfaces ethernets: # Network 1 eth0: addresses: # List of IP[v4,v6] addresses to assign to this interface - 10.54.48.60/23 # example: 10.20.30.5/24, fd00:10:6b50:5180::24/60 # Disable if not using IPv4 gateway4: "10.54.48.1" # Default IPv4 gateway – can move it to another interface, if desired (example: default gateway on eth2) # Enable if using IPv6 gateway6: "" # Default IPv6 gateway – you can move it to another interface if desired (example: default gateway on eth2)

7. Issue the `genisoimage` command to create the ISO file:

```
genisoimage -o etcd.iso -V cidata -r /tmp/etcd
```

8. After creating the ISO file, issue the following commands to remove the temporary `etcd` directory:

```
sudo umount /tmp/etcd
rm -rf /tmp/etcd
```

The ISO configuration is now complete.

9. Copy the `.iso` file created to the KVM host or VMWare Datasource.

Installing etcd on OpenStack

Start

1. Log on to the Ribbon Support portal. Download the Heat template file (`heat_template.yml`) and image file (`AppServices-<version>-<version>_vmCCS-<version>-x86_64.qcow2`). For more information on using the portal, refer to [Downloading Files from Ribbon Support Portal](#).
2. Create or re-use an existing flavor that specifies the recommended configuration (1 vCPU, 2GB of memory, 50GB of disk space). Refer to [Create an OpenStack Flavor](#).
3. Create a security group that defines "allow" rules for the following ingress and egress traffic. Refer to [Create a Security Group](#).

Port	Description
2381	etcd Prometheus exporter
9013	Nginx Prometheus exporter
9100	Prometheus node exporter (metrics)
9292	Backup-manager Prometheus exporter
9090	Prometheus
9093	Prometheus AlertManager client
9801	Service Discovery Representative (SDR) Prometheus exporter
9802	nf-operations exporter
9803	vnf-operations exporter

Port	Description
24231	Fluentbit Prometheus exporter
9094	Prometheus AlertManager cluster communication
2379	etcd client requests
2380	etcd peer communication

4. Configure an external network for your deployment. Refer to [Create an External Network](#).

Name	Description	Default
ext_net1	Public network with floating IP addresses for network 1. Used to allocate a floating IP to the instance.	EXT_OAM_0_STATIC

5. Create a etcd image on the Glance image server using the qcow2 image file you downloaded. Refer to [Create a Glance Image](#).
6. Use the OpenStack GUI to launch the etcd instance. On the **Launch Stack** window, use the following table to edit the following configurations, as needed, for your environment.

Parameter	Description	Mandatory	Example
image	Image to use for the etcd VM, use the image uploaded in step 5	Yes	AppServices-22.12.00A000-B4225_vmCCS-1.6.0-alpha-B2575-x86_64.qcow2
flavor	OpenStack flavour to use, use the flavour created at step 2	Yes	46fd3493-108e-456d-9c47-66a1ea95d699
security group	Security group to use for the VM, use the security group create at step 3	Yes	default
authorized key	SSH public keys authorized to connect to this VNF.	Yes	
availability zone	Network availability zone for this VNF.	No	
management interface hostname	Hostname to use for management interface.	No	ammanetcd
management interface domain name	Domain name to use for management interface.	No	local

Parameter	Description	Mandatory	Example
user root password	Password for the root user of the VNF instance.	No	Sonus@123
user sysadm password	Password for the <code>sysadm</code> user of the VNF instance. (<code>sysadm</code> is the administrative account)	Yes	Sonus@123
Etcd registries	VM communicate uses this function with the etcd cluster for network function coordination, for example to register this VM for monitoring. Information on how to reach the etcd cluster members and the options on how to fill this field are explained below: ◦ Recommended: Single entry pointing to an SRV FQDN that then points to all etcd instances. This is recommended because SRV records can be updated with topology changes. ◦ Empty: This will cause the VM to always communicate to the local etcd which has knowledge of the List of all planned members IPs.	No	
Existing VNF instances	IP addresses of any etcd instances created before.	Yes	fd00:10:6b50:61b0::4c7,fd00:10:6b50:61b0::1bc
etcd username	Name of an etcd user with read/write permissions to all keys related to VNF operations.	No	
etcd password	Password of for the etcd user with read/write permissions to all keys related to VNF operations.	No	

Parameter	Description	Mandatory	Example
Salt	Salt value for cryptography operations done during VNF operations. Ensure it is the same for all VMs of a deployment. Ribbon recommends making it unique per deployment.	No	
Use_etcd	Provide etcd as a service.	Yes	true
Use_prometheus	Provide Prometheus as a service.	Yes	true
Use_alertmanager	Provide Prometheus Alertmanager as a service.	Yes	true
Use_mongo	Provide a MongoDB server as a service.	Yes	False
etcd_data_volume_id	Identifier of the Cinder volume to use for etcd data.	No	
etcd_backup_volume_id	Identifier of the Cinder volume to use for etcd backup.	No	
etcd_root_password	Password for the ETCD root user. This user has all access to etcd including creation of users, policies, removing kes store etc.	No	
etcd_user_name	Username for a etcd user. This user has read/write permission on path with same name.	No	
etcd_user_password	Password for the etcd user.	No	
etcd_client_cert	etcd GRPC client certificate. Used for init and etcdctl commands.	No	
etcd_client_key	etcd GRPC client private key. Used for init and etcdctl commands.	No	
etcd_client_ca_cert	etcd GRPC client CA certificate. Used for init and etcdctl commands.	No	

Parameter	Description	Mandatory	Example
etcd_server_cert	etcd GRPC server certificate. Used for grpc server.	No	
etcd_server_key	etcd GRPC server private key. Used for grpc server.	No	
etcd_server_ca_cert	etcd GRPC server CA certificate. Used for grpc server.	No	
etcd_peer_cert	etcd GRPC peer certificate. Used for clustering.	No	
etcd_peer_key	etcd GRPC peer private key. Used for clustering.	No	
etcd_peer_ca_cert	etcd GRPC peer CA certificate. Used for clustering.	No	
etcd_heartbeat_interval	Interval in ms at which the leader will notify followers that it is still the leader.	No	
etcd_election_timeout	Describes how long in ms a follower node will go for without hearing a heartbeat before attempting to become leader itself.	No	
etcd_backup_disk_max_use	Maximum percentage of the disk that may be occupied by etcd backup files.	No	
etcd_backup_disk_keep_free	Percentage of disk that must be left free on the file system. The oldest backup files will be deleted when this limit is reached.	No	

Parameter	Description	Mandatory	Example
etcd_backup_start_time	Time of day when backup schedule starts in hh:mm+hh:mm or hh:mm-hh:mm format. First part of the format is the start time and second part is an offset (from UTC) for specifying the time zone. If the time zone is not specified, local time zone of the VM processing the request will be used as the default time zone.	No	
etcd_backup_full_period	Interval at which the etcd full backups are performed. Expressed in weeks and/or days, or hours format, e.g. 1w2d or 4h. Hours cannot be provided with days or weeks. Maximum value for hour is 23h. 0 means that no backup is performed.	No	
etcd_backup_retention	Time specifies how long to wait before deleting the file(s). Empty value means that we keep the files for 7 days. It is expressed in weeks, days and/or hours format, e.g. 1w24h or 2d.	No	
prometheus_data_volume_id	Identifier of the Cinder volume to use for Prometheus and/or AlertManager data.	No	
prometheus_max_disk_usage_in_percent	Maximum disk usage allowed by Prometheus data in percent of the total disk size.	No	
DNS nameserver(s)	Comma-separated list of DNS nameservers to use in the private subnet.	No	fd00:10:6b50:61c0::4d1,fd00:10:6b50:61c0::4d2
DNS search domains	Comma-separated list of DNS search domains to use in the private subnet.	No	rbbn.com
NTP server(s)	Comma-separated list of time servers to use for clock synchronization.	No	fd00:10:6b50:61c0::4d3

Parameter	Description	Mandatory	Example
NTP time zone	Time zone used for clock synchronization.	No	America/New_York
elasticsearch_host_addr	Remote Elasticsearch node's hostname or IP address. Used for log aggregation.	No	
elasticsearch_host_port	Remote Elasticsearch node port. Used for log aggregation.	No	
elasticsearch_index	Index name to use for Elasticsearch logging destination. Used for log aggregation.	No	
elasticsearch_http_user	Username credential for X-Pack access.	No	
elasticsearch_http_password	Password for user defined in HTTP_User.	No	
elasticsearch_tls_enable	Enable or disable TLS support.	Yes	Off
elasticsearch_tls_verify	Force certificate validation.	Yes	On
elasticsearch_record_type_filters	Comma-separated list of record type filter(s) to use for elasticsearch (tdr, log)	Yes	tdr, log
syslog_host_addr	Remote syslog node's hostname or IP address. Used for log aggregation.	Yes	10.54.21.201
syslog_host_port	Remote syslog node's port. Used for log aggregation.	Yes	514
syslog_protocol	Remote syslog node's transport protocol. Used for log aggregation.	Yes	"udp", "tcp", "tls"
syslog_record_type_filters	Comma-separated list of record type filter(s) to use for syslog (tdr, log)	Yes	tdr,log

Parameter	Description	Mandatory	Example
syslog_ca_cert	Remote syslog node's CA certificate. Used for sending logs over TLS (protocol set to 'tls'). Line breaks must be converted to '\n' - see user guide.	No	
fluent_host_addr	FluentD/Fluent Bit aggregator node hostname or IP address. Used for log aggregation.	No	
fluent_host_port	FluentD/Fluent Bit aggregator node port. Used for log aggregation.	No	
fluent_record_type_filters	Comma-separated list of record type filter(s) to use for FluentD/Fluent Bit aggregator node (tdr, log).	Yes	
ext_net1	Network 1 used to allocate an IP to the instance.	Yes	EXT_OAM_0_STATIC
use_net2	If true, add a second network interface.	Yes	False
ext_net2	Network 2 used to allocate an IP to the instance.	No	
use_net3	If true, add a third network interface.	Yes	False
ext_net3	Network 3 used to allocate an IP to the instance.	Yes	
default_net	Network on which default gateway is defined. This determines the interface which is assigned the 0.0.0.0/0 route in the server.	Yes	
management_net	Network used for configuration, management and metrics traffic. If network 2 or 3 are specified, they must be enabled.	Yes	1

Parameter	Description	Mandatory	Example
signaling_net	Network used for signaling traffic. If network 2 or 3 are specified, they must be enabled.	Yes	2
internal_net	Network used for database & application-internal traffic. If network 2 or 3 are specified, they must be enabled.	Yes	2
routes_net1	Comma-delimited list of destination subnets for which traffic should be sent through eth0 (network 1). These routes should align with the ingress networks configured above. Multiple routes may be specified as a comma-delimited list.	No	
routes_net2	Comma-delimited list of destination subnets for which traffic should be sent through eth1 (network 2). These routes should align with the ingress networks configured above. Multiple routes may be specified as a comma-delimited list.	No	
routes_net3	Comma-delimited list of destination subnets for which traffic should be sent through eth2 (network 3). These routes should align with the ingress networks configured above. Multiple routes may be specified as a comma-delimited list.	No	
service_registries	Comma-separated list of service registry servers to use for service discovery.	No	
dns_nameservers	Comma-separated list of DNS nameservers to use in private subnet.	No	
dns_search	Comma-separated list of DNS search domains to use in private subnet.	No	

Parameter	Description	Mandatory	Example
ntp_servers	Comma-separated list of time servers to use for clock synchronization.	Yes	10.128.254.67
time_zone	Time zone used for clock synchronization. Format: time zone database, e.g. 'America/New_York'	Yes	Asia/Kolkata
vnf_instances	Comma-separated list of existing VNF instance(s) IP address. The internal interface IPs of the previously instantiated instances in the AppServices cluster should be applied here.	No	
vnf_replace	Existing VNF instance IP address to replace. This new instance will replace the instance specified here.	No	
use_etcd	Provide etcd as a service.	True	
use_prometheus	Provide Prometheus as a service.	True	
use_alertmanager	Provide Prometheus Alertmanager as a service.	True	
backup_username	Defines a user that can access and retrieve the DB backup files.	Yes	backup_user
backup_user_password	Password for the backup user of the VNF instance. If left blank, user will not be created.	No	
backup_user_key	SSH public key authorized to connect to the backup user account. Use this parameter with caution in production settings.	No	
mongo_data_volume_id	Identifier of the Cinder volume to use for MongoDB data.	No	
mongo_backup_volume_id	Identifier of the Cinder volume to use for MongoDB backup.	No	

Parameter	Description	Mandatory	Example
mongo_authkey	Authentication key used to authenticate each MongoDB instances together. Only required when using password authentication.	No	MongoDB auth key must be between 6 and 1024 characters and use base64 characters only.
mongo_admin_password	Password for the MongoDB admin user. This user has read/write permissions in all databases. If this is left empty, MongoDB will be configured without authentication.	No	
mongo_user_name	Username for a MongoDB user. This user has read/write permissions on a database of the same name.	No	
mongo_user_password	Password for the MongoDB user. Allowed special characters are: !: [*._]~+-(){}^=/@#\$\$?;&`<>	No	
mongo_backup_disk_max_use	Maximum percentage of the disk that may be occupied by MongoDB backup files.	Yes	15
mongo_backup_disk_keep_free	Percentage of disk that must be left free on the file system. The oldest backup files will be deleted when this limit is reached.	Yes	30
mongo_backup_start_time	Time of day when backup schedule starts in hh:mm+hh:mm or hh:mm-hh:mm format. First part of the format is the start time and second part is an offset (from UTC) for specifying the time zone. If the time zone is not specified, local time zone of the VM processing the request will be used as the default time zone.	Yes	02:00

Parameter	Description	Mandatory	Example
mongo_backup_full_period	Interval at which the MongoDB full backups are performed. Expressed in weeks and/or days, or hours format, e.g. 1w2d or 4h. Hours cannot be provided with days or weeks. Maximum value for hour is 23h. 0 means that no backup is performed.	Yes	1d
mongo_backup_differential_period	Interval at which the MongoDB differential backups are performed. Expressed in weeks and/or days, or hours format, e.g. 1w2d or 4h. Hours cannot be provided with days or weeks. Maximum value for hour is 23h. 0 means that no backup is performed.	Yes	4h
mongo_backup_retention	Time specifies how long to wait before deleting the file(s). Empty value means that we keep the files for 7 days. It is expressed in weeks, days and/or hours format, e.g. 1w24h or 2d. When retention is more than a day, the extra hours of a day would be trimmed and retention value would be rounded down to the closest day.	No	
etcd_existing_endpoints	Comma-separated list of existing etcd endpoint(s) <scheme>://<host address>:<client port>. For etcd clustering, this will take precedence over 'Existing VNF instances'	No	
etcd_data_volume_id	Identifier of the Cinder volume to use for etcd data.	No	
etcd_backup_volume_id	Identifier of the Cinder volume to use for etcd backup.	No	
etcd_root_password	Password for the etcd root user. This user has all access to etcd including creation of users, policies, removing kes store etc.	No	

Parameter	Description	Mandatory	Example
etcd_user_name	Username for a etcd user. This user has read/write permission on path with same name.	No	
etcd_user_password	Password for the etcd user.	No	
etcd_client_cert	etcd GRPC client certificate. Used for init and etcdctl commands.	No	
etcd_client_key	etcd GRPC client private key. Used for init and etcdctl commands.	No	
etcd_client_ca_cert	etcd GRPC client CA certificate. Used for init and etcdctl commands.	No	
etcd_server_cert	etcd GRPC server certificate. Used for grpc server.	No	
etcd_server_key	etcd GRPC server private key. Used for grpc server.	No	
etcd_server_ca_cert	etcd GRPC server CA certificate. Used for grpc server.	No	
etcd_peer_cert	etcd GRPC peer certificate. Used for clustering.	No	
etcd_peer_key	etcd GRPC peer private key. Used for clustering.	No	
etcd_peer_ca_cert	etcd GRPC peer CA certificate. Used for clustering.	No	
etcd_heartbeat_interval	Interval in ms at which the leader will notify followers that it is still the leader.	Yes	100
etcd_election_timeout	How long in ms a follower node will go for without hearing a heartbeat before attempting to become leader itself.	Yes	1000

Parameter	Description	Mandatory	Example
etcd_backup_disk_max_use	Maximum percentage of the disk that may be occupied by etcd backup files.	Yes	15
etcd_backup_disk_keep_free	Percentage of disk that must be left free on the file system. The oldest backup files will be deleted when this limit is reached.	Yes	30
etcd_backup_start_time	Time of day when backup schedule starts in hh:mm+hh:mm or hh:mm-hh:mm format. First part of the format is the start time and second part is an offset (from UTC) for specifying the time zone. If the time zone is not specified, local time zone of the VM processing the request will be used as the default time zone.	Yes	02:00
etcd_backup_full_period	Interval at which the etcd full backups are performed. Expressed in weeks and/or days, or hours format, e.g. 1w2d or 4h. Hours cannot be provided with days or weeks. Maximum value for hour is 23h. 0 means that no backup is performed.	Yes	0
etcd_backup_retention	Time specifies how long to wait before deleting the file(s). Empty value means that we keep the files for 7 days. It is expressed in weeks, days and/or hours format, e.g. 1w24h or 2d.	No	
prometheus_data_volume_id	Identifier of the Cinder volume to use for Prometheus and/or AlertManager data.	No	
prometheus_max_disk_usage_in_percent	Maximum disk usage allowed by Prometheus data in percent of the total disk size.	Yes	40
snmp_trap_target_ip	snmp trap target address.	Yes	10.34.146.134

Parameter	Description	Mandatory	Example
snmp_trap_target_port	snmp trap target Port.	Yes	162

7. Click **Launch**.
A "Stack creation in progress message" appears.
Once the stack is created, the status changes to **Create Complete**.
8. Complete the remaining steps to verify the instantiation.
9. Click on **Stack Name** and verify that the Topology is up.
10. Wait approximately 10 minutes for the etcd to become accessible. To validate that services are running once the VM is ready, check the status of appservices using the following command as sysadm user.

```
$ vmccs-status
```

Example vmccs-status output:

```
$ vmccs-status
Validating backup-manager services status...
  backup-manager: active (running)
backup-manager is active

Validating Etcd services status...
  etcd: active (running)
Etcd is active

Validating Fluentbit services status...
  td-agent-bit: active (running)
  fluent-sd: active (running)
  fluent-sd-watch: active (running)
Fluentbit is active

Validating nginx services status...
  nginx: active (running)
  nginx-exporter: active (running)
nginx is active

Validating Node Exporter services status...
  node-exporter: active (running)
Node Exporter is active

Validating Prometheus services status...
  prometheus: active (running)
  prometheus-autoconfig: active (running)
  alertmanager: active (running)
  alertmanager-watch: active (running)
Prometheus is active
```

```
Validating SDR services status...
  sdr: active (running)
SDR is active

Validating VNF Operations services status...
  vnf-operations: active (running)
VNF Operations is active

All required vmCCS services are active.
```

Network **interface** roles

Default Gateway	Management	Internal	Signaling
eth0	eth0	eth0	eth0

11. To check the status of etcd cluster synchronization and health of any node, refer to [Health Check etcd](#).

Installing etcd on VMware

Create the etcd VMs Using the VMware GUI

Perform the following procedure on the Ribbon Application Management Platform (RAMP) to instantiate the etcd VMs using the VMware GUI.

Prerequisite

- Three free IPs are required to allocate to the etcd instances.
- The recommended configuration is one vCPU, 2 GB of memory, and a minimum of 50 GB of disk space. For more information, refer to [RAMP etcd System Requirements](#).
- Verify the network interfaces are connected and operable.
- Verify whether you have obtained the necessary installation files:
 - ISO configuration files
 - VMDK disk image filesFor more information on using the portal, refer to [Downloading Files from Ribbon Support Portal](#).
- Create customized ISO configuration drive for VMware. Refer to [Create an ISO Configuration Drive for VMware or KVM](#)

Start

1. Log on to the VMware ESXi GUI.
2. Upload the VMDK and ISO installation files to the VMware server using the VMware ESXi GUI:
 - a. In the left navigation menu, select **Storage**.
 - b. Under **Storage**, select a datastore device to which you want to upload.
 - c. Select **Datastore browser**.
 - d. Within the datastore, select an existing directory where you want to store the original images, or click **Create directory** to create a new directory for this purpose. **Example directory name:** etcdvnf-orig.

- e. In the target directory, select **Upload** and then navigate to one of the installation files and upload it. Select **Upload** again and repeat the process to locate and upload each VMDK and ISO file until you have uploaded all of the installation files.
- f. Check the Datastore browser status or check the VMware GUI's "Recent Tasks" pane to ensure that all of the uploads are completed before continuing.

The uploaded VMDK files are in a sparse format. Sparse disk images cannot be used directly to launch a VM; they must be converted to a flat format. Copying the files, as described in the following step, automatically converts them to the flat format required to launch a VM.

3. Create a copy of the appropriate VMDK image file (AppServices) for each VM you plan to deploy. Copies are essential because, during the VM creation process, the VMDK image file is transformed into a disk image. This means you cannot reuse the same file to create another VM instance. To launch multiple VM instances, you need to make a copy of the original VMDK image file for each instance. Each time you create a copy, the VMDK file is automatically converted into a flat VMDK file, which can then be used to launch a VM.

To copy a VMDK image file:

- a. In the **Datastore browser**, select an original VMDK file that was uploaded and select **Copy**.
- b. Select an existing folder that you want to hold the active VM disk images or click **Create directory** to create a new directory for this purpose. Example directory name: etcdvnf.
- c. Name the image file copies appropriately according to the type of VM they will launch. Ribbon recommends to include the version in the name to avoid confusion during upgrade. Examples: vmappetcd1_23.02.00R000.vmdk, vmappetcd2_23.02.00R000.vmdk.
- d. Repeat the previous steps to copy an original VMDK image file for each VM that you plan to launch.

4. Create the first VM.

Note

These instructions apply to all the VMs: first to the first Services VM, then to the second and third Services VMs.

Refer to [RAMP etcd System Requirements](#) for the CPU, memory (RAM), hard disk and host OS requirements of each VM.

- a. Create the new VM.
From the VMware GUI home menu, use the menus to create a new VM.
 - i. Select *Virtual Machines -> Create / Register VM -> Create a new virtual machine*.
 - ii. Click **Next** to continue.
 - iii. In the **Select a name and guest OS** menu:
 1. Provide the host name for the VM.
Example host name for the first Services VM: `vmappetcd1`
 2. Select the Operating System (OS).
Example: Compatibility ESXi 6.7 virtual machine, Guest OS Family Linux, Guest OS Version Red Hat Enterprise Linux 8 (64-bit).
 - iv. Click **Next** to continue.
 - v. In the **Select storage** menu:

1. If the Standard and Persistent Memory options appear, select **Standard** for the storage type.
 2. Choose the appropriate datastore for the VM's configuration files and virtual disks.
Example datastore name: datastore1, Capacity: 500 GB, Free: 460 GB, Type: VMFS6, Thin provisioning: Supported, Access: Single
 - vi. Click **Next** to continue.
- b. Customize the new VM.
- In the **Customize settings** menu, configure the VM hardware.
- i. Select the **VM Options** tab.
 1. Click **Boot options** from the list.
 2. Select **BIOS** for Firmware.
 - ii. Select the **Virtual Hardware** tab.
 - iii. Configure the VM CPU and memory.
 Example configurations:
 1. Select **1 CPU and 2 GB RAM** for a Services VM.
 - iv. Set up the VMDK (Virtual Machine Disk) hard drive.
 1. Delete the default hard disk (Hard disk 1) by selecting the "X" next to it.
 2. Select **Add hard disk**.
 3. In the pop-up window select **Existing hard disk**.
 4. In the **Datastore browser** window, browse the datastore folder and select the file corresponding to the appropriate VMDK file you created earlier.
 - a. Example file name if creating a Services VM: vmappetcd1.vmdk (or vmappetcd2.vmdk or vmappetcd3.vmdk)
 5. Click **Select** to continue.
 6. Change the **Controller location** (or "Virtual Device Node") and "Virtual Device Node unit" to **IDE controller 0** and **Master**.
 7. Click the expand/contract triangle of the **New Hard disk** list to contract the list and make the rest of the **Customize settings** visible.
 - v. Set up the ISO configuration drive.

Warning

Even after initial installation, the configuration drive must remain mounted.

1. On the CD/DVD Drive change the drop down to **Datastore ISO file**.
 2. In the **Datastore browser** window, browse the datastore folder and select the file corresponding to the appropriate ISO file you transferred earlier.
 - a. Example file name if creating a Services VM:
 vmappetcd1.iso (or vmappetcd2.iso or vmappetcd3.iso if creating the second or third Services VM)
 3. Click **Select** to continue.
 - vi. **Configure Networking**.
 Select the appropriate network.
- c. Finish creating the new VM and power it on.
- i. Click **Next** in the **Customize settings** menu to continue.
 - ii. In the **Ready to complete** menu, review the settings you have selected.
 - iii. Click **Finish** to complete the creation of the VM.
 - iv. Power on (activate) the VM.
 In the list of Virtual Machines, right-click the VM you just created.
 Select *Power* -> *Power on*.

- v. Verify the services that are running on the VM. After about ten minutes, run the `vmccs-status` command from the SSH login to verify all services are running on the VM.
5. To check the status of etcd cluster synchronization and health of any node, refer to [Health Check etcd](#).

Upgrading etcd

In this section:

- [Upgrading etcd on KVM](#)
- [Upgrading etcd on VMware](#)
- [Upgrading etcd on Openstack](#)
- [Upgrading etcd on Kubernetes](#)

The software upgrade of the Services VMs consists of rebuilding each VM and allowing each VM's database member to re-synchronize with the rest of the database. Since the VM being upgraded reuses the same IP address, and the addresses of the other VM nodes remain the same, no further intervention is required; re-synchronization occurs automatically.

Throughout the upgrade procedures, the following naming conventions apply:

- **appetcd1**, **appetcd2**, and **appetcd3** represent the three Application and Database Services VMs (referred to as Services VMs).

You can replace those names with host names or any other specific names you choose, as long as you maintain consistency throughout the steps. However, Ribbon recommends that you rename the files to the above naming conventions when copying the files to the host server to make it easier to follow the procedure examples.

Additionally, Ribbon recommends including the release version in the file name to distinguish one release version from another. For example:

- **APPETCD1_[release version]**
- **APPETCD2_[release version]**
- **APPETCD3_[release version]**

Overall Flow

A high-availability model requires a minimum of three Services VMs, each hosting a replication member. The three members form a quorum, and the quorum selects a Primary member and a Leader.

In the overall flow, you upgrade the three Services VMs – A, B, and C – in the following order.

Step	Description	Services VMs
		bold = upgraded * = Primary (or Leader)
1	Initial state of the replica set	A*, B, C
2	Rebuild member C	A*, B, C

Step	Description	Services VMs
3	1. Forcefully step down A as Primary and promote C as the new Primary. 2. Confirm that the system behavior is correct.	A, B, C*
4	Rebuild member B	A, B , C*
5	Rebuild member A	A , B , C*

Note

When the configuration includes more than three replication members (more than three Services VMs), remember this:

- You upgrade the additional members in the same manner as the first ones: one at a time rebuild each VM and allow its replication member to re-synchronize before upgrading the next VM.
- Repeating Step 3 to forcefully step down another Primary member is not necessary; the overall upgrade strategy only requires the forced step down of the Primary once.

Upgrading etcd on KVM

Use the following procedure to upgrade etcd on KVM.

Note

During the upgrade of a KVM-based Services VM, you will work with the following files:

- the QCOW2 disk image file
- the UPGRADE_APPETCD1[or 2 or 3].iso file, which is the upgrade cloud-init customized configuration drive (.iso) file.

The examples show commands for the first Services VM, APPETCD1. For subsequent VMs, substitute APPETCD2 or APPETCD3 as appropriate.

Prerequisites

- Check the status of the etcd cluster. Refer to [Validate Health Check etcd](#).
- To download the files for etcd Installation, refer to [Downloading Files for ETCD Installation on KVM](#).

Start

1. Create a temporary variable named `$etcd_storage_path`. Create a sub-directory under it named `orig`. Use the storage path variable in this session only, as an aid to placing the installation files on the KVM host. The sub-directory holds the QCOW2 file.
 - a. Log on to the host server.
 - b. Enter this command: `export etcd_storage_path=/var/lib/libvirt/storage/etcd`
 - c. Confirm by entering this command: `echo $etcd_storage_path`
 - d. Create a sub-directory named `orig`: `$etcd_storage_path/orig/`
2. Create a customized ISO configuration drive for KVM. Refer to [Create an ISO Configuration Drive for VMware or KVM Upgrade](#).

3. Transfer the new QCOW2 image file and the new customized configuration drive (.iso) file for the Services VM to the KVM host server.

For more information on obtaining the QCOW2 files, refer to [Download Files for etcd Installation on KVM](#).

Attention

Be sure to select the "upgrade" version of the customized configuration drive (.iso) file, the one that does not reinitialize the database replication. This will assume replication is already in place and the upgraded VM only needs to be re-synchronized to the existing replica set.

- i. Place the QCOW2 file in the *orig* sub-directory: `$etcd_storage_path/orig/`.
- ii. Place the "upgrade" configuration drive (.iso) file in the `$etcd_storage_path` directory.

4. Create a copy of the QCOW2 file.

During the VM creation, the QCOW2 image file becomes a disk image, and you cannot use the same file again to create another VM instance. Hence, to launch more than one VM instance, you must create a new QCOW2 image file for each VM instance. Include the release version in the name of the copy so you can distinguish it from earlier versions.

Example file names of the copies:

APPETCD1_[release version].qcow2 for the first Services VM

APPETCD2_[release version].qcow2 for the second Services VM

APPETCD3_[release version].qcow2 for the third Services VM

Example command for APPETCD1:

Example output:

```
$ cp $etcd_storage_path/orig/[AppServices-release_specific_file.qcow2]
$etcd_storage_path/APPETCD1_[ release version ].qcow2
```

5. Destroy the VM.

Execute the following command. Enter the VM name (APPETCD1, APPETCD2, or APPETCD3) as appropriate:

```
$ sudo virsh shutdown <VM name>
```

Repeat the following command until the response shows that the VM is shut down:

```
$ sudo virsh list --all
```

Once the VM is shut down, enter the following command:

```
$ sudo virsh undefine <VM name>
```

6. Launch the Services VM.

Use the following command as an example. The example assumes certain values mentioned earlier, such as the storage paths. Detailed parameters depend on the user's environment.

- The command includes the addition of a `--disk` argument for the persistent storage volume created during the initial installation of the VM.
- The QCOW2 image dictates the values of the `--os-type` and `--os-variant` parameters.
- The `--network` argument passed in the example below assumes the use of bridges called `br-vms` and `br-data` as the VNF's network interface. If that is not the case (using a custom bridge or libvirt network), adapt the argument accordingly.
- If choosing to deploy with one network interface, remove one of the `--network` arguments.
- Ribbon does not support deploying a VM with more than one network interface using the same bridge.

Example command for APPETCD1 (use APPETCD2 or APPETCD3 for subsequent Services VMs):

Example output:

```
export VNF_NAME=ammanetcd # Replace with your desired VM name

sudo virt-install \

  --name $VNF_NAME \
  --memory 2048 \
  --disk $etcd_storage_path/APPETCD1_[ release
version ].qcow2,device=disk,bus=virtio \
  --disk $etcd_storage_path/
UPGRADE_APPETCD1.iso,device=disk,bus=virtio,readonly=on \
  --os-type linux \
  --os-variant rhel8.2 \
  --graphics none \
  --network bridge=br0,model=virtio \
  --import I am running a few minutes late; my previous meeting is running over.
```

Note

The VM boots and runs several post installation tasks.

- During these tasks the VM reboots.
The console continues to provide updates. The final update reads:
"finish: modules-final: SUCCESS: running modules for final"
Several lines above this a report appears indicating if any failures occurred:
"Ran 10 modules with 0 failures"
- If a login prompt appears with "localhost", contact Ribbon Support. Otherwise, log in with user account *sysadm*.

7. Use `sudo bash` and check for the system listening on port 27017 using `netstat -an | grep 0.0.0.0:27017`.

Example output:

```
[sysadm@5n-appdb1 ~]$ sudo bash
[root@5n-appdb1 sysadm]# netstat -an | grep 0.0.0.0:27017
tcp        0      0 0.0.0.0:27017      0.0.0.0:*          LISTEN
```

8. Verify the etcd instance has re-synchronized. For more information, refer to [Health Check etcd](#).

Upgrade the additional members similar to the first one. Rebuild each VM, one at a time and allow its replication member to re-synchronize before upgrading the next VM.

For the etcd upgrade sequence, refer to [Upgrading etcd](#).

Create an ISO Configuration Drive for VMware or KVM Upgrade

Use this procedure to create an ISO configuration drive to upgrade VMware or KVM on the Ribbon Application Management Platform (RAMP).

Start

1. Log on to the Ribbon Support portal. Download the `AppServices-configDrive.img` files. For more information on using the portal, refer to [Download Files from Ribbon Support Portal](#).
2. Log on to a Linux server as the `root` user. On this server, create an `.iso` file from the provided template file, `AppServices-configDrive.img` to use as a configuration drive for the Virtual Machine (VM).
3. Create a temporary directory. In the following example the directory name is "etcd":

```
mkdir -p /tmp/etcd
```

4. Mount the image:

```
sudo mount AppServices-configDrive.img /tmp/etcd
```

5. Use the following command to edit the cloud configuration. Refer to the table for parameter information.

```
vim /tmp/etcd/user-data
```

Cloud Configuration Parameters

Parameters To Edit	Description	Example	Note
hostname	Hostname of the VM in use	hostname: "amman etcd"	

Parameters To Edit	Description	Example	Note
fqdn	FQDN of the VM in use	fqdn: "ammanetcd.local"	
timezone	Choose the time zone	timezone: "Asia/Kolkata"	
ntp	NTP server IP	servers: ["10.128.254.67"]	

Parameters To Edit	Description	Example	Note
VnfName GatewayIpv4/ GatewayIpv6 ExternalIp	hostname: ammanetcd1 VnfName: amman- ramp-geo-cluster Gateway IP address of the etcd instance Externally visible IP address of the ETCD instance.	# Ribbon vmCCS userdata: - content: { "VnfName": "amman-ramp-geo- cluster",	◦ Net{1,2,3}: Definition for the interface IF{1,2,3} ◦ Enabled : Indicates if the interface is enabled. Enabled is mandatory. You must set it to "true" or "false". ◦ GatewayIpv4: IPv4 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface ◦ GatewayIpv6: IPv6 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface ◦ ExternalIp: External IP address for this interface ◦ Categories: List of category of traffic on this interface. By default, management is on net1, signaling and internal are on net2, and nothing is configured for net3. ◦ IsDefault: Indicates whether or not to assign the default route to this interface. Only one interface may have IsDefault=true. If false for all interfaces, the first interface with a gateway configured is assigned the default route. This parameter is not required if only one gateway was specified in the network-config file.

Parameters To Edit	Description	Example	Note
		<pre> "Networks": { "Net1": { "Enabled": "True", "GatewayIpv4": "", "GatewayIpv6": "fd00:10:6b50:40c0:: 1", "Externallp": "fd00:10:6b50:40c0:: 24", "Categories": [], "IsDefault": "True" }, "Net2": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "Externallp": "", "Categories": [], "IsDefault": "" }, "Net3": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "Externallp": "", "Categories": [], "IsDefault": "" } }, </pre>	

Parameters To Edit	Description	Example	Note
Etcd	Etcd configuration	<pre> "Etcd": { "ExistingEndpoints" : [], "PersistentDataPath" : "", "PersistentBackupPath" : "", "RootPassword" : "", "UserName" : "", "UserPassword" : "", "ClientCert" : "", "ClientKey" : "", "ClientCaCert" : "", "ServerCert" : "", "ServerKey" : "", "ServerCaCert" : "", "PeerCert" : "", "PeerKey" : "", "PeerCaCert" : "", "HeartbeatInterval" : "", "ElectionTimeout" : "", "BackupDiskMaxUse" : "", "BackupDiskKeepFree" : "", "BackupStartTime" </pre>	◦ PersistentDataPath: Path to the persistent disk to use for Etcd data. The virtio number corresponds to the Etcd data volume ID provided in the deployment. ◦ RootPassword: The Etcd database password for the root user. If left blank, no authentication is enabled on the database. In a HA setup, the passwords must match on all the virtual machines. ◦ UserName: The name of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank. ◦ UserPassword: The password of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank. ◦ HeartbeatInterval: The interval (in ms) at which the leader notifies followers that it is still the leader. The recommended value to set is around the maximum of average round-trip time (RTT) between members, it is normally around 0.5-1.5x the round-trip time. If this field is left blank or omitted, the default value is 100 ms.

Parameters To Edit	Description	Example	Note
		<pre> : "", "BackupFullPeriod" : "0", "BackupRetention" : "" }, </pre>	◦ ElectionTimeout: The duration (in ms) that a follower node performs without hearing a heartbeat before attempting to become the leader. The recommended value to set must be at least 10 times the RTT to account for a variance in the network. If this field is left blank or omitted, the default value is 1000 ms. ◦ BackupDiskMaxUse: The maximum percentage of the disk that allowed to be occupied by the Etcd backup files. The default value is 15. ◦ BackupDiskKeepFree: The percentage of disk that must be left free on the file system. The oldest backup files are deleted when this limit is reached. The default value is 30. ◦ BackupStartTime: The time of day when the scheduled backup starts. The format is in hh:mm±hh:mm. The first part of the format is the start time and second part is an offset (from UTC) to specify the time zone. If the time zone is not specified, then the local time zone of the virtual machine processing the request is used as the default time zone. The default value is 02:00.

Parameters To Edit	Description	Example	Note
			◦ BackupFullPeriod : The interval at which a full backup of the Etcd full is performed. This is expressed in the format of weeks and/or days, or hours. For example, 1w2d or 4h. Hours are not allowed to be provided with days or weeks. • The maximum allowed value for hours is 23h. • The minimum allowed value is 1h. • 0 means that no backup is performed. The default value is 1d. Note Set the BackupFullPeriod as 0 (Zero). ◦ BackupRetention : Specifies how long the backup files are retained before deleting the file(s). An empty value means that the backup files are retained for 7 days. This is expressed in the format of weeks, days and/or hours. For example, 1w24h or 2d.

Parameters To Edit	Description	Example	Note
EtcdRegistries	Information to connect to the ETCD cluster	<pre>"VnfOperations": { "EtcdRegistries": [, "EtcdUserName": "admin", "EtcdUserPassword" : "admin", "Salt": "mysalt@123"</pre>	VM communicate uses this function with the ETCD cluster for network function coordination, for example to register this VM for monitoring. Information on how to reach the ETCD cluster members and the options on how to fill this field are explained below: ◦ Recommended : Single entry pointing to an SRV FQDN that then points to all ETCD instances. This is recommended because SRV records can be updated with topology changes. ◦ Empty : This will cause the VM to always communicate to the local ETCD which has knowledge of the List of all planned members IPs.
VnfExistingInstances	IP addresses of any etcd instances created before	<pre>"VnfExistingInstances": ["10.54.8.166","10.54.8.165","10.54.8.167"], "VnfReplaceInstance" : "", "UseMongoDB" : "", "UseEtcd" : "True", "UsePrometheus" : "True", "UseAlertManager" : "True",</pre>	While creating the ETCD instance, "VnfExistingInstances" must contain the IP address of all the three etcd instances.

Parameters To Edit	Description	Example	Note
Prometheus	Prometheus configuration	"Prometheus": { "PersistentDataPath" : "", "MaxDiskUsage" : "40" }	Prometheus configuration Fields: - PersistentDataPath: Path to the persistent disk to use for Prometheus and AlertManager data. The virtio number corresponds to the Prometheus data volume ID provided in the deployment. - MaxDiskUsage: Maximum disk usage allowed by Prometheus data in percent of the total disk size.

Example etcd Userdata

```
#cloud-config

# Hostname to use for this VM
hostname: "ammanetcd"

# FQDN to use for this VM, usually just <hostname>.local
fqdn: "ammanetcd.local"

# DO NOT CHANGE
preserve_hostname: false

# DO NOT CHANGE
manage_etc_hosts: true

# List of groups to create on this VM
groups:
  # User part of this group can read backup files
  - backup_group # This group name is used by ansible during the VM initial
    configuration

# List of users to create/update on this VM
users:
  # Recommended user for systems administrators
  - name: root
    plain_text_passwd: "Sonus@123"
    lock_passwd: false

  - name: sysadm
    plain_text_passwd: "shipped!!"
    lock_passwd: false
```

```

    ssh_authorized_keys:
      - "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAqJX+iihNxOPZNHwBXbEogknmUH2xvupn8/
bcx9YmAT7RcVsJ4ICMIGic1yAJjhdRWgTRwpGqBKzftUVanBZS232aBETPMGZHgTdpjpFdUMGHiYU4niwmmw
Gzp84mnyZoqwh5pGau9ZTJL2IUjyh0t7a/s2RXHu88HHC4+SduD5fWiU0GL0bc8re2lXdkUIlk/
Sg430GNqHW68SnZI7yPWZJbv9z3+6qN2oxvBqd/
eb9RbQQzoupSci0BFBkYhUiRFbNQZAcTF7+4XFkraSnBLtYckN+EPDJv4G/
Uk9bi65320g5SQPFoXEzenk2STLJq0tiCcMeX04fIw0bhC0SgQ== ssequeira@ptbats"

# Timezone for this VM (format: tz database, e.g. "America/New_York")
timezone: "Asia/Kolkata"

# List of NTP servers to use on this VM
ntp:
  servers: ["10.128.254.67"]
  ntp_client: chrony # DO NOT CHANGE
  config:
    service_name: chronyd # DO NOT CHANGE

# Files that will be written to disk
write_files:
  # DO NOT CHANGE
  - content: |
      {
        "TemplateName": "heat_template.yaml"
      }
    path: /opt/rbbsn/userData.json
    owner: root:root
    permissions: '0600'

# Ribbon vmCCS userdata: fill in all fields according to user guide
- content: |
    {
      "VnfName": "amman-ramp-geo-cluster",

      "Networks": {
        "Net1": {
          "Enabled": "True",
          "GatewayIpv4": "",
          "GatewayIpv6": "",
          "ExternalIp": "172.19.52.209",
          "Categories": [],
          "IsDefault": "true"
        },
        "Net2": {
          "Enabled": "False",
          "GatewayIpv4": "",
          "GatewayIpv6": "",
          "ExternalIp": "",
          "Categories": [],
          "IsDefault": "false"
        }
      },
    },

```

```
"Net3": {
  "Enabled": "False",
  "GatewayIpv4": "",
  "GatewayIpv6": "",
  "ExternalIp": "",
  "Categories": [],
  "IsDefault": "false"
}
},

"VnfOperations": {
  "EtcdRegistries": [],
  "EtcdUserName": "",
  "EtcdUserPassword": "",
  "Salt": ""
},

"ServiceDiscovery": {
  "RegistryType": "dns",
  "Registries": []
},

"Logging": {
  "Elasticsearch": {
    "Hosts": [{
      "Addr": "",
      "Port": "",
      "HttpUser": "",
      "HttpPasswd": "",
      "TlsEnable": "Off",
      "TlsVerify": "On",
      "RecordTypeFilters": ["tdr","log"]
    }],
    "Index": ""
  },
  "Syslog": {
    "Hosts": [{
      "Addr": "10.54.21.201",
      "Port": "514",
      "RecordTypeFilters": ["tdr","log"]
    }],
    "Protocol": "udp",
    "CACert": ""
  },
  "Fluent": {
    "Hosts": [{
      "Addr": "",
      "Port": "",
      "RecordTypeFilters": ["tdr","log"]
    }],
  }
},
},
```

```

    "Metrics": {
        "Export": "True"
    }
}
path: /etc/rbbn/podman/userdata.json
owner: root:root
permissions: '0600'

# Ribbon AppServices userdata: fill in all fields according to user guide
- content: |
{
  "VnfExistingInstances" : ["172.19.52.139","172.19.52.129","172.19.52.209"],
  "VnfReplaceInstance"   : "",
  "UseMongoDB"           : "False",
  "UseEtcd"               : "True",
  "UsePrometheus"        : "True",
  "UseAlertManager"      : "True",

  "MongoDB": {
    "PersistentDataPath"      : "",
    "PersistentBackupPath"    : "",
    "AuthKey"                 : "",
    "AdminPassword"           : "",
    "UserName"                : "",
    "UserPassword"            : "",
    "BackupDiskMaxUse"        : "15",
    "BackupDiskKeepFree"     : "30",
    "BackupStartTime"         : "02:00",
    "BackupFullPeriod"        : "1d",
    "BackupDifferentialPeriod" : "4h",
    "BackupRetention"         : ""
  },

  "Etcd": {
    "ExistingEndpoints"       : [],
    "PersistentDataPath"      : "",
    "PersistentBackupPath"    : "",
    "RootPassword"           : "",
    "UserName"                : "",
    "UserPassword"            : "",
    "ClientCert"              : "",
    "ClientKey"               : "",
    "ClientCaCert"            : "",
    "ServerCert"              : "",
    "ServerKey"               : "",
    "ServerCaCert"            : "",
    "PeerCert"                : "",
    "PeerKey"                 : "",
    "PeerCaCert"              : "",
    "HeartbeatInterval"       : "100",
    "ElectionTimeout"         : "1000",
    "BackupDiskMaxUse"        : "15",
    "BackupDiskKeepFree"     : "30",

```

```

        "BackupStartTime"      : "02:00",
        "BackupFullPeriod"    : "0",
        "BackupRetention"     : ""
    },

    "Prometheus": {
        "PersistentDataPath" : "",
        "MaxDiskUsage"      : "40"
    }
}
path: /etc/rbbn/appservices/userdata.json
owner: root:root
permissions: '0600'

# DO NOT CHANGE
runcmd:
    # Launch main vmCCS playbook (downstream plays are launched by this playbook)
    - ansible-playbook /etc/rbbn/podman/configure.yml

```

6. Edit the network configuration:

```
vim /tmp/etcd/network-config
```

Edit the following parameters in the `network-config` file:

Parameters to edit	Description	Example
addresses	IP address to assign to this interface.	# DO NOT CHANGE version: 2 # List of network interfaces ethernets: # Network 1 eth0: addresses: # List of IP[v4,v6] addresses to assign to this interface - 10.54.48.60/23 # example: 10.20.30.5/24, fd00:10:6b50:5180::24/60 # Disable if not using IPv4 gateway4: "10.54.48.1" # Default IPv4 gateway – can move it to another interface, if desired (example: default gateway on eth2) # Enable if using IPv6 # gateway6: "" # Default IPv6 gateway – you can move it to another interface if desired (example: default gateway on eth2)
gateway4/gateway6	The default IP gateway.	

7. Use the `genisoimage` command to create the ISO file:

```
genisoimage -o etcd.iso -V cidata -r /tmp/etcd
```

8. After creating the ISO file, remove the temporary `etcd` directory:

```
sudo umount /tmp/etcd
rm -rf /tmp/etcd
```

The ISO configuration is now complete.

9. Copy the `.iso` file created to the KVM host or VMware Datasource.

Upgrading etcd on VMware

Use the following procedure to upgrade the etcd on VMware.

Prerequisites

- Check the status of the etcd cluster. Refer to Validate [Health Check etcd](#).

Start

1. Log on to the VMware ESXi GUI.
2. For instructions on obtaining the VMDK image file and customized drive (ISO) files, refer to [Download Files from Ribbon Support Portal](#). Unless there is a specific counter-indication, the ISO configuration drives from a prior etcd version remain compatible with the new version and do not have to be updated. For any specific VMDK file names, refer to the [Latest Release Notes](#).
3. Create a customized ISO configuration drive for VMware. Refer to [Create an ISO Configuration Drive for VMware or KVM Upgrade](#).
4. Upload the VMDK and ISO installation files to the VMware server using the VMware ESXi GUI:
 - a. In the left navigation menu, select **Storage**.
 - b. Under **Storage**, select a datastore device you want to upload.
 - c. Select the **Datastore browser**.
 - d. Within the datastore, select an existing directory where you want to store the original images or click **Create a directory** to create a new directory for this purpose.
Example directory name: `stivnf-orig`
 - e. In the target directory, select **Upload**, navigate to one of the installation files, and upload it. Select **Upload again**, and repeat the process to locate and upload each VMDK and ISO file (if applicable) until you have uploaded all of the installation files.
 - f. Before continuing, check the Datastore browser status or the VMware GUI's "Recent Tasks" pane to ensure that all of the uploads have been completed.

Warning

The uploaded VMDK files are in a sparse format. Sparse disk images cannot be used directly to launch a VM; they must be converted to a flat format. Copying the files, as described in the following step, automatically converts them to the flat format required to launch a VM.

5. Create a copy of the AppServices VMDK image file for each Services VM you plan to upgrade. Copies are necessary because, during the VM creation process, the VMDK image file becomes a disk image. Therefore, you cannot use the same file again to create another VM instance. To launch more than one VM instance, you must make a copy of the original VMDK image file for each VM instance you plan to launch. As you create each copy, the VMDK file is automatically converted into a flat VMDK file that can

be used to launch a VM.

To copy a VMDK image file:

- a. In the **Datastore browser**, select an original uploaded VMDK file and choose **Copy**.
 - b. Select an existing folder that you want to hold the active VM disk images or click **Create directory** to create a new directory. Example directory name:
stivnf
 - c. Name the image file copies appropriately according to the type of VM they will launch. Ribbon recommends including the version in the name to avoid confusion during the upgrade. Examples: vmappetcd1_23.02.00R000.vmdk, vmappetcd2_23.02.00R000.vmdk, vmwappdb3_23.02.00R000.vmdk
 - d. Repeat the previous steps to copy an original VMDK image file for each Services VM you plan to upgrade.
6. Shut down the VM.
Select [**your VM**]> **Actions**> **Power**> **Power off**.
 7. Replace the VMDK file.
 - a. Go to **Edit settings** in the Actions menu and remove the existing VMDK file in the hard drive list.
 - b. Click **Save**.
 - c. In the Action menu, add the new VMDK file. For settings, refer to [Installing etcd on VMware](#).
Example of new VMDK file: `vmwappetcd1_[ release version ].vmdk`
 8. Replace the ISO configuration drive.
 - a. On the CD/DVD Drive, change the drop-down to "Datastore ISO file."
 - b. In the "Datastore Browser" window, browse the datastore folder and select the file corresponding to the ISO file you uploaded earlier in Step 4.
Example file name: UPGRADE_vmwappdb1.iso

Attention

Be sure to select the "upgrade" version of the customized configuration drive (.iso) file, the one that does not reinitialize the database replication. This will be the one that assumes replication is already in place and the upgraded VM only needs to re-synchronize to the existing replica set.

- c. Click [**Select**] to continue.
9. Power on the VM.
Select [**your VM**]> **Actions**> **Power**> **Power on**.
10. Verify the instance has re-synchronized. For more information, refer to [Health Check etcd](#).

Note

Upgrade the additional members similar to the first one. Rebuild each VM, one at a time and allow its replication member to re-synchronize before upgrading the next VM.

For etcd upgrade sequence, refer to [Upgrading etcd](#).

Upgrading etcd on Openstack

Use the following procedure to upgrade etcd on Openstack.

Prerequisites

- Log on to the Ribbon Support Portal to download the `heat_template_etcd.yml` and `AppServices-
<version>-<version>_vmCCS-<version>-x86_64.qcow2` files.
Refer to [Download Files from Ribbon Support Portal](#).
- Create a Glance Image for the new etcd version.
Refer to [Create a Glance Image](#).

Start

1. Check the status of the etcd Cluster.
Refer to [Health Check etcd](#).
2. Complete the following to delete the existing stack of the etcd instance.
 - a. Using the OpenStack Dashboard GUI, shut off the etcd instance:
 - i. Navigate to **Project > Instances**.
 - ii. Select the **etcd** instance from the drop-down menu.
 - iii. Select **Shut off instance**.
 - b. Delete the stack of the etcd instance.
 - i. Click **Project > Orchestration > Stacks**. Select the **etcd** stack for the instance you want to terminate and click **Delete Stacks**.
 - ii. Confirm the deletion when prompted.
 - c. Instantiate an etcd instance to be the active instance with the following:
 - Identical stack name and hostname.
Refer to [Installing etcd on OpenStack](#).
3. Verify the instance has re-synchronized.
For more information, refer to [Health Check etcd](#).

Note

Upgrade the additional members similar to the first one. Rebuild each VM, one at a time, and allow its replication member to re-synchronize before upgrading the next VM.
For the etcd upgrade sequence, refer to [Upgrading etcd](#).

Upgrading etcd on Kubernetes

Use the following procedure to upgrade etcd on Kubernetes.

Prerequisites

- Three free IP addresses are available to allocate to the etcd instances.
- Ensure the platforms use RCP 5.4.3 and/or OCP RH-openshift 4.10.18 or later versions.
- Review [RAMP etcd System Requirements](#) to ensure your environment has the necessary resources and prerequisite software available.

Start

1. Log on to the Ribbon Support portal and download the HELM chart for etcd. For more information, refer to [Download Files from Ribbon Support Portal](#).
2. Untar the HELM chart:

```
tar -xvf <name of the Helm chart>.tar
```

3. Change the directory:

```
cd etcd/
```


4. Edit the values in the `yaml` file:

```
vi values.yaml
```

For more information on etcd parameters, refer to [etcd Parameters](#).

5. Install the HELM chart after editing the values in the `.yaml` file:

```
helm upgrade <deployment name> --values values.yaml .
```

An example of `values.yaml`

Example

```
## @section Global parameters
## Please, note that this will override the image parameters, including
## dependencies, configured to use the global value
##
global:
  ## @param global.imageRegistry Containers image registry
  ##
  imageRegistry: "artifact2.eng.sonusnet.com"
  ## @param global.imagePullSecrets [array] Global Docker registry secret names as
  ## an array
  ## E.g.
  ## imagePullSecrets:
  ##   - name: myRegistryKeySecretName
  ## Note: for backwards compatibility, directly specifying the secrets as a list
  ## of strings without the name: attribute is also supported, but not recommended
  ##
  imagePullSecrets: ["sanramp-imagecred"]
  ## @param global.imagePullSecretsTemplate [array]
  ## Template strings to evaluate to existing secret to use to pull images, for
  ## example: name: "{{.Release.Name }}-imagecred"
  ##
  imagePullSecretsTemplate: []
  ## @param imageCredentials Create image pull credentials
  ##
  imageCredentials:
    name: "ssequira-8"
    registry: artifact2.eng.sonusnet.com
    username: ssequira
    password:
eyJ2ZXIiOiIyIiwidHlwIjoislUiiwiYXNjoiUlMyNTYiLCJraWQiOiJ0b2Z0emxGZGtnSjdaWFnRn
RTTm94RzBLMTE3ZEZldEVAxVXd5YVg3a2xVIn0.eyJzdWIiOiJqZnJ0QDAXY2RyYnJwejljYzclMXFnemI5
bTlxaHBLXC91c2Vyc1wvc3NlcXVlaXJhIiwic2NwIjoibWVtYmVyLW9mLWdyb3Vwc3pyZWZkZXJzIiwiaXNz
VkIjoiamZydEAgIiwiaXNzIjoiamZydEAWMTM0MiwiaWF0IjoxNzA2MDY1MzQyLCJqdGkiOiJmZWFlNjI0ZS0yMz
ZXF1ZWlyYSIsImV4cCI6MTczNzYwMTM0MiwiaWF0IjoxNzA2MDY1MzQyLCJqdGkiOiJmZWFlNjI0ZS0yMz
IwLTRhZDEtOGM5Mi0xMzUyNzI5MDc0NzkiZjQ.Z_E60050KSvANFBXMoQeJBQLBSr3taxE1xhZQmDWQx6Yj
0u7pW1rt6-P6kaECuSFf7X-
xqBxqAKUr8TBbzq20n8DyrQoCfuqAv5UcD77TAE4H1290p1HhHtcs3f7f10dwiEhNDA932X0EGAIATHPI1
```

```

yWqx3qcaD849FbPq18bZFWNzXYBNkhABZ4g_gn6j8IUEj5yjdBNXn_b3JFzIfvH6hwyXBgaMCXDtSzbH6g
jvMMLUq9lC9GTlxv7qhnhqB5uMRumlVuv4X0BUVKtFDsk3EEEfQFV4I-
xsFd66iEkR03qI7s063Xsopfoq_KipwUPP5pSsPHks3B7NyN2dqxiA
  ## @param global.serviceAccount to use for pods
  ##
  serviceAccount:
    ## @param global.serviceAccount.name Name of the service account to use
    ##
    name: ""
  ## @param global.storageClass Global StorageClass for Persistent Volume(s)
  ##
  storageClass: ""
  ## Cert-manager information to use in the csi-driver volume
  ##
  certManager:
    ## @param global.certManager.enabled Switch to enable the use of cert-manager
    to manage certificates
    ##
    enabled: true
    issuer:
      ## @param global.certManager.issuer.name The Issuer name to sign the
      certificate request
      ##
      name: "cross-cluster-ca-selfsigned-clusterissuer"
      ## @param global.certManager.issuer.kind The Issuer kind to sign the
      certificate request. Can be "Issuer" or "ClusterIssuer"
      ## See https://cert-manager.io/docs/concepts/issuer/ for more information
      ##
      kind: "ClusterIssuer"
  ## @param global.ns_uuid Global NS UUID
  ##
  ns_uuid: "ns_uuid"
  ## @param global.cnf_uuid Global CNF UUID
  ##
  cnf_uuid: "cnf_uuid"
  ## @param global.cnfc_uuid Global CNFC UUID
  ##
  cnfc_uuid: "cnfc_uuid1"
  ## @param global.kubernetesPlatform K8s platform type: "oc" or "robin"
  ##
  kubernetesPlatform: ""
  ## @param global.obs parameters
  ##
  obs:
    ## @param global.obs.image image parameters
    ##
    image:
      ## @param global.obs.image.repository observability agent image name
      ##
      repository: "ccs-docker-prod-virtual/rbbn_telemetry_collector"
      ## @param global.obs.image.tag observability agent image tag
      ##
      tag: "3.1.1"

```

```

    ## @param global.obs.image.pullPolicy observability agent image pull policy.
Defaults to 'Always' if image tag is 'latest', else set to 'IfNotPresent'
    ##
    pullPolicy: IfNotPresent
    ## @param global.obs.logPersistentVolumeStorage settings for log PVC
    ##
    logPersistentVolumeStorage:
    ## @param global.obs.logPersistentVolumeStorage.request Size of the PVC
storage request
    ##
    request: 20Gi
    ## @param global.obs.logs parameters
    ##
    logs:
    ## @param global.obs.logs.telemetry log telemetry config
    telemetry:
    ## @param global.obs.logs.telemetry.topic telemetry logs will be sent to
this Kafka topic
    topic: rbbn-otel-agent
    ## @param global.obs.logs.backendServers log backends
    ##
    backendServers: {}
    ## @param obs.logs.backendServers.elasticsearch elasticsearch backend
    ## Warning: username and password represent the name of the ENV variable
name
    ## that contains the username and password from the secret
    # elasticsearch:
    #   - endpoint: <elasticsearch server address>:443
    #     auth: True
    #     username: ELASTICSEARCH_USER
    #     password: ELASTICSEARCH_PASSWD
    #     index: <filebeat index>
    ## @param obs.logs.backendServers.kafka kafka backend
    ##
    # kafka:
    #   - endpoint: <kafka server address>:<kafka port>
    #     sslCert: KAFKA_CERT
    #     sslKey: KAFKA_KEY
    #     sslCa: KAFKA_CA
    ## @param global.obs.logs.elasticsearchSecretName name of common
elasticsearch credentials secret
    ##
    elasticsearchSecretName: ""
    ## @param obs.logs.kafkaSecretName Name of secret containing Kafka
environment variables
    ## Evaluated as a template, for example: "{{ .Release.Name }}-elasticsearch-
user-creds"
    #
    elasticsearchSecretNameTemplate: ""
    ## @param global.obs.logs.elasticsearchSecretName name of common kafka
credentials secret
    ##
    kafkaSecretName: ""

```

```

    ## @param obs.global.logs.kafkaSecretName Name of secret containing Kafka
    environment variables
    ## Evaluated as a template, for example: "{{ .Release.Name }}-kafka-user-
    creds"
    ##
    kafkaSecretNameTemplate: ""

    ## @param global.prometheusRule Prometheus alerting rules
    ##
    prometheusRule:
    ## @param global.prometheusRule.create Specifies whether a PrometheusRule
    resource should be created
    ##
    # create: false
    ## @param global.prometheusRule.labels Specify additional labels so the
    Prometheus instance can discover the rules
    ##
    labels: {}

    ## @param global.customizedResourcePrefix template definitions for resource name
    prefixes
    ##
    customizedResourcePrefix:
    servicePrefixTemplate: ""
    configmapPrefixTemplate: ""

    persistence:
    ## @param global.persistence.annotations Annotations to add to the
    PersistentVolumeClaims
    ##
    annotations: {}

    ## @param global.terminationMessagePolicy Container termination message policy
    ## https://kubernetes.io/docs/tasks/debug/debug-application/determine-reason-
    pod-failure/
    terminationMessagePolicy: "FallbackToLogsOnError"
    ## @param global.tolerations [array] Tolerations for pod assignment
    ## Ref: https://kubernetes.io/docs/concepts/configuration/taint-and-toleration/
    ##
    tolerations: []

    ## @section Common parameters

    ## @param kubeVersion Force target Kubernetes version (using Helm capabilities if
    not set)
    ##
    kubeVersion: ""
    ## @param nameOverride String to partially override etcd.fullname template (will
    maintain the release name)
    ##
    nameOverride: ""
    ## @param fullnameOverride String to fully override etcd.fullname template
    ##

```

```

fullnameOverride: ""
## @param commonLabels [object] Labels to add to all deployed objects
##
commonLabels: {}
## @param commonAnnotations [object] Annotations to add to all deployed objects
##
commonAnnotations: {}
## @param clusterDomain Default Kubernetes cluster domain
##
clusterDomain: cluster.local
## @param extraDeploy [array] Array of extra objects to deploy with the release
##
extraDeploy: []

## @section roles parameters
##
roles:
  ## @param roles.create Enable/disable Role and RoleBinding creation. If set to
  ## false, the ServiceAccount passed in global will need the following rules:
  ## If using a NodePort service:
  ## - apiGroups: ["" ] # "" indicates the core API group
  ##   resources: ["services"]
  ##   verbs: ["get"]
  ## If using persistence:
  ## - apiGroups: ["" ]
  ##   resources: ["persistentvolumeclaims"]
  ##   verbs: ["get", "list", "delete", "deletecollection"]
  ##
  create: false

## Enable diagnostic mode in the deployment
##
diagnosticMode:
  ## @param diagnosticMode.enabled Enable diagnostic mode (all probes will be
  ## disabled and the command will be overridden)
  ##
  enabled: false
  ## @param diagnosticMode.command [array] Command to override all containers in
  ## the deployment
  ##
  command:
    - sleep
  ## @param diagnosticMode.args [array] Args to override all containers in the
  ## deployment
  ##
  args:
    - infinity

## @param imageRegistryPath Containers image repository path in the registry
##
imageRegistryPath: "/dockerhub-docker-remote"

## @section etcd parameters

```

```

## etcd image version
## ref: https://console.cloud.google.com/gcr/images/etcd-development/GLOBAL/etcd
## ref: https://hub.docker.com/r/bitnami/etcd/tags/
## @param image.repository etcd image name
## @param image.tag etcd image tag
## @param image.pullPolicy etcd image pull policy
##
image:
  repository: bitnami/etcd
  tag: 3.5.13
  ## Specify a imagePullPolicy
  ## Defaults to 'Always' if image tag is 'latest', else set to 'IfNotPresent'
  ## ref: https://kubernetes.io/docs/user-guide/images/#pre-pulling-images
  ##
  pullPolicy: IfNotPresent
  ## Set to true if you would like to see extra information on logs
  ##
  debug: false
## kubectl image (used for init and cleanup)
## ref: https://hub.docker.com/r/bitnami/kubectl/tags/
## @param kubectl.image.repository kubectl image name
## @param kubectl.image.tag kubectl image tag
##
kubectl:
  image:
    repository: bitnami/kubectl
    tag: 1.30.1
## Authentication parameters
##
auth:
  ## Role-based access control parameters
  ## ref: https://etcd.io/docs/current/op-guide/authentication/
  ##
  rbac:
    ## @param auth.rbac.create Switch to enable RBAC authentication
    ##
    create: false
    ## @param auth.rbac.allowNoneAuthentication Allow to use etcd without
    configuring RBAC authentication
    ##
    allowNoneAuthentication: true
    ## @param auth.rbac.rootPassword Root user password. The root user is always
    `root`
    ##
    rootPassword: ""
    ## @param auth.rbac.existingSecret Name of the existing secret containing
    credentials for the root user
    ##
    existingSecret: ""
    ## @param auth.rbac.existingSecretPasswordKey Name of key containing password
    to be retrieved from the existing secret
    ##

```

```

    existingSecretPasswordKey: ""
    ## Authentication token
    ## ref: https://etcd.io/docs/latest/learning/design-auth-v3/#two-types-of-tokens-simple-and-jwt
    ##
    token:
      ## @param auth.token.type Authentication token type. Allowed values: 'simple'
      or 'jwt'
      ## ref: https://etcd.io/docs/latest/op-guide/configuration/#--auth-token
      ##
      type: jwt
      ## @param auth.token.privateKey.filename Name of the file containing the
      private key for signing the JWT token
      ## @param auth.token.privateKey.existingSecret Name of the existing secret
      containing the private key for signing the JWT token
      ## NOTE: Ignored if auth.token.type=simple
      ## NOTE: A secret containing a private key will be auto-generated if an
      existing one is not provided.
      ##
      privateKey:
        filename: jwt-token.pem
        existingSecret: ""
      ## @param auth.token.signMethod JWT token sign method
      ## NOTE: Ignored if auth.token.type=simple
      ##
      signMethod: RS256
      ## @param auth.token.ttl JWT token TTL
      ## NOTE: Ignored if auth.token.type=simple
      ##
      ttl: 10m
    ## TLS authentication for client-to-server communications
    ## ref: https://etcd.io/docs/current/op-guide/security/
    ##
    client:
      ## @param auth.client.secureTransport Switch to encrypt client-to-server
      communications using TLS certificates
      ##
      secureTransport: true
      ## @param auth.client.useAutoTLS Switch to automatically create the TLS
      certificates
      ##
      useAutoTLS: false
      ## @param auth.client.existingSecret Name of the existing secret containing
      the TLS certificates for client-to-server communications
      ##
      existingSecret: ""
      ## @param auth.client.enableAuthentication Switch to enable host
      authentication using TLS certificates. Requires existing secret
      ##
      enableAuthentication: true
      ## @param auth.client.certFilename Name of the file containing the client
      certificate
      ##

```

```

    certFilename: cert.pem
    ## @param auth.client.certKeyFilename Name of the file containing the client
certificate private key
    ##
    certKeyFilename: key.pem
    ## @param auth.client.caFilename Name of the file containing the client CA
certificate
    ## If not specified and `auth.client.enableAuthentication=true` or
`auth.rbac.enabled=true`, the default is is `ca.crt`
    ##
    caFilename: "ca.pem"
    ## @param auth.client.certDuration Requested duration the signed certificate
will be valid for
    ##
    certDuration: ""
    ## @param auth.client.certExtraDnsSans DNS Subject Alternative Name to add to
the certificates
    ##
    certExtraDnsSans: ""
    ## @param auth.client.certExtraIpSans IP Subject Alternative Name to add to
the certificates
    ##
    certExtraIpSans: ""
    ## TLS authentication for server-to-server communications
    ## ref: https://etcd.io/docs/current/op-guide/security/
    ##
    peer:
        ## @param auth.peer.secureTransport Switch to encrypt server-to-server
communications using TLS certificates
        ##
        secureTransport: true
        ## @param auth.peer.useAutoTLS Switch to automatically create the TLS
certificates
        ##
        useAutoTLS: false
        ## @param auth.peer.existingSecret Name of the existing secret containing the
TLS certificates for server-to-server communications
        ##
        existingSecret: ""
        ## @param auth.peer.enableAuthentication Switch to enable host authentication
using TLS certificates. Requires existing secret
        ##
        enableAuthentication: true
        ## @param auth.peer.certFilename Name of the file containing the peer
certificate
        ##
        certFilename: cert.pem
        ## @param auth.peer.certKeyFilename Name of the file containing the peer
certificate private key
        ##
        certKeyFilename: key.pem
        ## @param auth.peer.caFilename Name of the file containing the peer CA
certificate

```



```

    ## If not specified and `auth.peer.enableAuthentication=true` or
`rbac.enabled=true`, the default is is `ca.crt`
    ##
    caFilename: "ca.pem"
    ## @param auth.peer.certDuration Requested duration the signed certificate
will be valid for
    ##
    certDuration: ""
    ## @param auth.peer.certExtraDnsSans DNS Subject Alternative Name to add to
the certificates
    ##
    certExtraDnsSans: ""
    ## @param auth.peer.certExtraIpSans IP Subject Alternative Name to add to the
certificates
    ##
    certExtraIpSans: ""
    ## @param autoCompactionMode Auto compaction mode, by default periodic. Valid
values: "periodic", "revision".
    ## - 'periodic' for duration based retention, defaulting to hours if no time unit
is provided (e.g. 5m).
    ## - 'revision' for revision number based retention.
    ##
    autoCompactionMode: ""
    ## @param autoCompactionRetention Auto compaction retention for mvcc key value
store in hour, by default 0, means disabled
    ##
    autoCompactionRetention: ""
    ## @param heartbeatInterval Cluster leader heartbeat interval, in ms (by default
100)
    ## Refer to https://etcd.io/docs/v3.5/tuning/#time-parameters
    ##
    heartbeatInterval: ""
    ## @param electionTimeout Timeout after which a follower will start an election
when not receiving a leader heartbeat, in ms (by default 1000)
    ## Refer to https://etcd.io/docs/v3.5/tuning/#time-parameters
    ##
    electionTimeout: ""
    ## @param clusterName Cluster name - this is the name of the etcd cluster.
    ##
    clusterName: "sanetcd"
    ## @param existingEndpoints Existing cluster endpoints to use for bootstrapping.
    ## When this is set, the etcd instance created by this chart will add itself as a
member of the cluster.
    ## An example is: "https://etcd1:2379,https://etcd2:2379"
    ##
    existingEndpoints: ""
    ## @param initialCluster Initial cluster configuration for bootstrapping.
    ## When existingEndpoints is specified, this parameter is ignored.
    ## If existingEndpoints and this parameter are not specified, etcd will default to
"default=http://localhost:2380"
    ## An example is: "etcd1=https://etcd1:2380,etcd2=https://
etcd2:2380,etcd3=https://etcd3:2380"
    ##

```

```

initialCluster: ""
## @param initialClusterState Initial cluster state. Allowed values: 'new' or
'existing'.
## If this values is not set, the default values below are set:
## - 'new': when installing the chart ('helm install ...')
## - 'existing': when upgrading the chart ('helm upgrade ...') or when
existingEndpoints is set
##
initialClusterState: ""
## @param discoverySrv DNS SRV domain used to bootstrap the cluster.
## ref: https://etcd.io/docs/v3.5/op-guide/clustering/#dns-discovery
##
discoverySrv: ""
## @param discoverySrvName Suffix to the DNS SRV name queried when bootstrapping
using DNS.
## ref: https://etcd.io/docs/v3.5/op-guide/clustering/#dns-discovery
##
discoverySrvName: ""
## @param memberCount Number of etcd member(s) to deploy. Maximum value: 3.
## WARNING: This parameter MUST NOT be modified during an upgrade. Modifying this
value will cause the etcd member(s) to be restarted,
## potentially causing an unrecoverable loss of quorum.
##
memberCount: 1
## @param maxProcs Limits the number of operating system threads that can execute
user-level
## Go code simultaneously by setting GOMAXPROCS environment variable
## ref: https://golang.org/pkg/runtime
##
maxProcs: ""
## @param removeMemberOnUninstall Use a pre-delete chart hook to remove the etcd
member from the etcd cluster on chart uninstall
##
removeMemberOnUninstall: true
## @param configuration etcd configuration. Specify content for etcd.conf.yml
## e.g:
## configuration: |-
##     foo: bar
##     baz:
##
configuration: ""
## @param existingConfigmap Existing ConfigMap with etcd configuration
## NOTE: When it's set the configuration parameter is ignored
##
existingConfigmap: ""
## @param extraEnvVars [array] Extra environment variables to be set on etcd
container
## e.g:
## extraEnvVars:
##   - name: FOO
##     value: "bar"
##
extraEnvVars: []

```

```

## @param extraEnvVarsCM Name of existing ConfigMap containing extra env vars
##
extraEnvVarsCM: ""
## @param extraEnvVarsSecret Name of existing Secret containing extra env vars
##
extraEnvVarsSecret: ""
## @param command [array] Default container command (useful when using custom
images)
##
command: []
## @param args [array] Default container args (useful when using custom images)
##
args: []

## @section etcd statefulset parameters

statefulset:
  ## @param statefulset.enabled create statefulset if equal true
  ##
  enabled: true

## Update strategy
## ref: https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/
#update-strategies
## @param updateStrategy.type Update strategy type, can be set to RollingUpdate or
onDelete.
##
updateStrategy:
  type: RollingUpdate
## @param podManagementPolicy Pod management policy for the etcd statefulset
## ref: https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/
#pod-management-policies
##
podManagementPolicy: Parallel
## @param hostAliases [array] etcd pod host aliases
## ref: https://kubernetes.io/docs/concepts/services-networking/add-entries-to-
pod-etc-hosts-with-host-aliases/
##
hostAliases: []
## @param lifecycleHooks [object] Override default etcd container hooks
##
lifecycleHooks: {}
## etcd container ports to open
## @param containerPorts.client Client port to expose at container level
## @param containerPorts.peer Peer port to expose at container level
##
containerPorts:
  client: 2379
  peer: 2380
## etcd pods' Security Context
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/security-context/
#set-the-security-context-for-a-pod
## @param podSecurityContext.enabled Enabled etcd pods' Security Context

```

```

## @param podSecurityContext.fsGroup Set etcd pod's Security Context fsGroup
##
podSecurityContext:
  enabled: true
  fsGroup: 1001
## etcd containers' SecurityContext
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/security-context/
##set-the-security-context-for-a-container
## @param containerSecurityContext.enabled Enabled etcd containers' Security
Context
## @param containerSecurityContext.runAsUser Set etcd container's Security Context
runAsUser
## @param containerSecurityContext.runAsNonRoot Set etcd container's Security
Context runAsNonRoot
##
containerSecurityContext:
  enabled: true
  runAsUser: 1001
  runAsNonRoot: true
## etcd containers' resource requests and limits
## ref: https://kubernetes.io/docs/user-guide/compute-resources/
## We usually recommend not to specify default resources and to leave this as a
conscious
## choice for the user. This also increases chances charts run on environments
with little
## resources, such as Minikube. If you do want to specify resources, uncomment the
following
## lines, adjust them as necessary, and remove the curly braces after 'resources:'.
## @param resources.limits [object] The resources limits for the etcd container
## @param resources.requests [object] The requested resources for the etcd
container
##
resources:
  limits:
    cpu: 1
    memory: 2Gi
  requests:
    cpu: 1m
    memory: 128Mi
## Configure extra options for liveness probe
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-
liveness-readiness-startup-probes/#configure-probes
## @param livenessProbe.enabled Enable livenessProbe
## @param livenessProbe.initialDelaySeconds Initial delay seconds for
livenessProbe
## @param livenessProbe.periodSeconds Period seconds for livenessProbe
## @param livenessProbe.timeoutSeconds Timeout seconds for livenessProbe
## @param livenessProbe.failureThreshold Failure threshold for livenessProbe
## @param livenessProbe.successThreshold Success threshold for livenessProbe
##
livenessProbe:
  enabled: true
  initialDelaySeconds: 300

```

```

periodSeconds: 30
timeoutSeconds: 5
successThreshold: 1
failureThreshold: 5
## Configure extra options for readiness probe
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/#configure-probes
## @param readinessProbe.enabled Enable readinessProbe
## @param readinessProbe.initialDelaySeconds Initial delay seconds for
readinessProbe
## @param readinessProbe.periodSeconds Period seconds for readinessProbe
## @param readinessProbe.timeoutSeconds Timeout seconds for readinessProbe
## @param readinessProbe.failureThreshold Failure threshold for readinessProbe
## @param readinessProbe.successThreshold Success threshold for readinessProbe
##
## BE CAREFUL!!! If using a Service, traffic will not be sent to the Pods until
they are Ready.
## This can lead to a deadlock where the etcd members cannot communicate and start
the cluster.
##
readinessProbe:
  enabled: false
  initialDelaySeconds: 10
  periodSeconds: 10
  timeoutSeconds: 5
  successThreshold: 1
  failureThreshold: 5
## Configure extra options for liveness probe
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-liveness-readiness-startup-probes/#configure-probes
## @param startupProbe.enabled Enable startupProbe
## @param startupProbe.initialDelaySeconds Initial delay seconds for startupProbe
## @param startupProbe.periodSeconds Period seconds for startupProbe
## @param startupProbe.timeoutSeconds Timeout seconds for startupProbe
## @param startupProbe.failureThreshold Failure threshold for startupProbe
## @param startupProbe.successThreshold Success threshold for startupProbe
##
startupProbe:
  enabled: false
  initialDelaySeconds: 0
  periodSeconds: 10
  timeoutSeconds: 5
  successThreshold: 1
  failureThreshold: 60
## @param customLivenessProbe [object] Override default liveness probe
##
customLivenessProbe: {}
## @param customReadinessProbe [object] Override default readiness probe
##
customReadinessProbe: {}
## @param customStartupProbe [object] Override default startup probe
##
customStartupProbe: {}

```

```

## @param extraVolumes [array] Optionally specify extra list of additional volumes
for etcd pods
##
extraVolumes: []
## @param extraVolumeMounts [array] Optionally specify extra list of additional
volumeMounts for etcd container(s)
##
extraVolumeMounts: []
## @param initContainers [array] Add additional init containers to the etcd pods
## e.g:
## initContainers:
##   - name: your-image-name
##     image: your-image
##     imagePullPolicy: Always
##     ports:
##       - name: portname
##         containerPort: 1234
##
initContainers: []
## @param sidecars [array] Add additional sidecar containers to the etcd pods
## e.g:
## sidecars:
##   - name: your-image-name
##     image: your-image
##     imagePullPolicy: Always
##     ports:
##       - name: portname
##         containerPort: 1234
##
sidecars: []
## @param podAnnotations [object] Annotations for etcd pods
## ref: https://kubernetes.io/docs/concepts/overview/working-with-objects/
annotations/
##
podAnnotations: {}
## @param podLabels [object] Extra labels for etcd pods
## Ref: https://kubernetes.io/docs/concepts/overview/working-with-objects/labels/
##
podLabels: {}
## @param podLabelsTemplate [object] Extra labels for etcd pods that can contain
variables
##
podLabelsTemplate: {}
## @param affinity [object] Affinity for pod assignment
## Ref: https://kubernetes.io/docs/concepts/configuration/assign-pod-node/
#affinity-and-anti-affinity
##
affinity: {}
## @param nodeSelector [object] Node labels for pod assignment
## Ref: https://kubernetes.io/docs/user-guide/node-selection/
##
nodeSelector: {}
## @param tolerations [array] Tolerations for pod assignment

```

```

## Ref: https://kubernetes.io/docs/concepts/configuration/taint-and-toleration/
##
tolerations: []
## @param terminationGracePeriodSeconds Seconds the pod needs to gracefully
terminate
## ref: https://kubernetes.io/docs/concepts/containers/container-lifecycle-hooks/
#hook-handler-execution
##
terminationGracePeriodSeconds: ""
## @param schedulerName Name of the k8s scheduler (other than default)
## ref: https://kubernetes.io/docs/tasks/administer-cluster/configure-multiple-
schedulers/
##
schedulerName: ""
## @param priorityClassName Name of the priority class to be used by etcd pods
## Priority class needs to be created beforehand
## Ref: https://kubernetes.io/docs/concepts/configuration/pod-priority-preemption/
##
priorityClassName: ""
## @param topologySpreadConstraints Topology Spread Constraints for pod assignment
## https://kubernetes.io/docs/concepts/workloads/pods/pod-topology-spread-
constraints/
## The value is evaluated as a template
##
topologySpreadConstraints: []

## @section Service exposing the etcd member outside the Kubernetes cluster

service:
  ## @param service.type Kubernetes Service type. Supported value: "NodePort" and
  "LoadBalancer"
  ## Note: There is always a headless service enabled to expose the etcd member
  within the Kubernetes cluster
  ##
  type: ""
  ## @param service.enabled create service to expose etcd outside a Kubernetes
  cluster in combination with sdrp-operator if equal true
  ##
  enabled: false
  ## @param service.dualStack exposes the service on both IPv4 and IPv6 if
  available when set to true
  ##
  dualStack: false
  ## @param service.clusterIP Kubernetes service Cluster IP
  ## e.g.:
  ## clusterIP: None
  ##
  clusterIP: ""
  ## @param service.ports.client etcd client port
  ## @param service.ports.peer etcd peer port
  ##
  ports:
    client: 2379

```

```

    peer: 2380
    ## @param service.nodePorts.client Specify the nodePort client value for the
    LoadBalancer and NodePort service types.
    ## @param service.nodePorts.peer Specify the nodePort peer value for the
    LoadBalancer and NodePort service types.
    ## ref: https://kubernetes.io/docs/concepts/services-networking/service/#type-
nodeport
    ##
    nodePorts:
      client: ""
      peer: ""
    ## @param service.loadBalancerIP loadBalancerIP for the etcd service (optional,
    cloud specific)
    ## ref: https://kubernetes.io/docs/user-guide/services/#type-loadbalancer
    ##
    loadBalancerIP: ""
    ## @param service.loadBalancerSourceRanges [array] Load Balancer source ranges
    ## ref: https://kubernetes.io/docs/tasks/access-application-cluster/configure-
cloud-provider-firewall/#restrict-access-for-loadbalancer-service
    ## e.g:
    ## loadBalancerSourceRanges:
    ##   - 10.10.10.0/24
    ##
    loadBalancerSourceRanges: []
    ## @param service.externalIPs [array] External IPs
    ## ref: https://kubernetes.io/docs/concepts/services-networking/service/
#external-ips
    ##
    externalIPs: []
    ## @param service.externalTrafficPolicy %%MAIN_CONTAINER_NAME%% service external
    traffic policy
    ## ref http://kubernetes.io/docs/tasks/access-application-cluster/create-
external-load-balancer/#preserving-the-client-source-ip
    ##
    externalTrafficPolicy: Cluster
    ## @param service.extraPorts Extra ports to expose (normally used with the
    `sidecar` value)
    ##
    extraPorts: []
    ## @param service.labels [object] Additional labels for the etcd service
    ##
    labels: {}
    ## @param service.annotations [object] Additional annotations for the etcd
    service
    ##
    annotations: {}
    ## @param service.sessionAffinity Session Affinity for Kubernetes service, can
    be "None" or "ClientIP"
    ## If "ClientIP", consecutive client requests will be directed to the same Pod
    ## ref: https://kubernetes.io/docs/concepts/services-networking/service/
#virtual-ips-and-service-proxies
    ##
    sessionAffinity: None

```



```

## @param service.sessionAffinityConfig Additional settings for the
sessionAffinity
## sessionAffinityConfig:
##   clientIP:
##     timeoutSeconds: 300
##
sessionAffinityConfig: {}
## @param service.sdrpScope When using sdrp-operator, this is the scope where
the SRV record is published.
## The A/AAAA record will always be published in the cluster scope.
## Allowed value: "global" or "cluster"
## Depending on this value, also configure "sdrpClusterDomain" or
"sdrpGlobalDomain" to enable automation
## of the configuration of the peer urls of this member with the fqdn of this
service published by sdrp-operator.
##
sdrpScope: "global"
## @param service.sdrpClusterDomain Cluster domain where the service is
published when using sdrp-operator
## This allow generating a fqdn representing the service globally.
## Required to allow geo-distributed etcd cluster when using a service of type
"LoadBalancer".
##
sdrpClusterDomain: ""
## @param service.sdrpGlobalDomain Global domain where the service is published
when using sdrp-operator
## This allow generating a fqdn representing the service globally.
##
sdrpGlobalDomain: ""
## @param service.sdrpClientFqdnInstance Overrides the instance part of the FQDN
for the etcd client SRV record published for the service.
## When it is used: <k8s service name>._<type>._<protocol>.<domain> ->
<instance>._<type>._<protocol>.<domain>
## Fill this with the same in every Helm release when deploying multiple
instances of this chart (i.e. multicluster)
## to publish SRV records for all instances under the same FQDN
sdrpClientFqdnInstance: ""
## @param service.extraFqdns [array] Extra fqdn(s) representing this service
## When cert-manager is generating certificates, this fqdn(s) will be added in
the certificate SAN.
## This fqdn(s) will also be added to the etcd member advertised url(s). The
fqdn(s) MUST be resolvable,
## otherwise, the etcd member will be unusable.
## NOTE: When using a service of type "LoadBalancer" and not using the sdrp-
operator, this allow providing
## a fqdn representing the load balancer.
## NOTE: When using a service of type "NodePort", this allow providing node(s)
fqdn. You will need to manually
## update the etcd member to add the peer urls based on this fqdn(s) once a port
is assigned.
##
extraFqdns: []

```

```

## @section networkInterface
## Using pod network interface for etcd communications
## When using TLS it is mandatory to either provide static ip or configure sdrp
operator
## For using sdrp operator, the interface, sdrpScope and sdrpClusterDomain values
should be provided
## For using static ip, the ip value should be defined
##
networkInterface:
  ## @param networkInterface.name selected network interface information for etcd
communication
  ## Etcd will be exposed through the selected network interface
  ## It should be chosen according to the name defined in networkAnnotation in the
networkAnnotations section
  ## To enable using the network interface the name of available network should be
provided
  ##
  name: 'ext-static-net-1'
  ## @param networkInterface.interface This is the name of interface that etcd
will be exposed through.
  ## This variable should be provided when using sdrp operator
  ##
  interface: 'net1'
  ## @param networkInterface.ip The ip that etcd will be exposed through.
  ## This variable should be specified when using static ip deployment
  ##
  ip: '10.52.154.136'
  ## @param networkInterface.disableIPv6Autoconfig If true, auto-config will be
disabled (only for ipv6)
  ## warning: enabling this parameter will force etcd chart to run sysctl command
in privileged mode.
  ## suggestion: disable ipv6 autoconfig by placing sysctl in a tuning cni plugin
section of the NetworkAttachmentDefinition.
  ##
  disableIPv6Autoconfig: false
  ## @param networkInterface.mtu This is to apply the mtu to the network interface
  ##
  mtu: ''
  ## @param networkInterface.addressIndex Index of IP address to use from attached
network
  ## For example, can be used for selecting an IPv6 address on a dual-stack
network
  ##
  addressIndex: 0
  ## @param networkInterface.defaultRoute This is the optional variable that will
be provided to k8s.v1.cni.cncf.io/networks annotation of pod
  ## It will be assigned to the "default-route" of k8s.v1.cni.cncf.io/networks
annotation
  ##
  defaultRoute: '10.52.154.1'
  ## @param networkInterface.namespace This is the optional variable that will be
provided to k8s.v1.cni.cncf.io/networks annotation of pod

```

```

    ## It will be assigned to the "namespace" of k8s.v1.cni.cncf.io/networks
    annotation
    ##
    namespace: ''
    ## @param networkInterface.sdrpScope When using sdrp-operator, this is the scope
    where the SRV record is published.
    ## The A/AAAA record will always be published in the cluster scope.
    ## Allowed value: "global" or "cluster"
    sdrpScope: ''
    ## @param networkInterface.sdrpClusterDomain domain where the network interface
    is published when using sdrp-operator in the scope
    ## This allow generating a fqdn representing the network interface in the scope.
    ## this is the variable that shows to use the sdrp.
    sdrpClusterDomain: ''
    ## @param service.sdrpClientFqdnInstance Overrides the instance part of the FQDN
for the etcd client SRV record published for the service.
    ## When it is used: <k8s service name>._<type>._<protocol>.<domain> ->
    <instance>._<type>._<protocol>.<domain>
    ## Fill this with the same in every Helm release when deploying multiple
    instances of this chart (i.e. multicluster)
    ## to publish SRV records for all instances under the same FQDN
    sdrpClientFqdnInstance: ''

## @section Persistence parameters

## Enable persistence using Persistent Volume Claims
## ref: https://kubernetes.io/docs/user-guide/persistent-volumes/
##
persistence:
    ## @param persistence.enabled If true, use a Persistent Volume Claim. If false,
    use emptyDir.
    ##
    enabled: true
    ## @param persistence.storageClass Persistent Volume Storage Class
    ## If defined, storageClassName: <storageClass>
    ## If set to "-", storageClassName: "", which disables dynamic provisioning
    ## If undefined (the default) or set to null, no storageClassName spec is
    ## set, choosing the default provisioner. (gp2 on AWS, standard on
    ## GKE, AWS & OpenStack)
    ##
    storageClass: ""
    ##
    ## @param persistence.annotations [object] Annotations for the PVC
    ##
    annotations: {}
    ## @param persistence.accessModes Persistent Volume Access Modes
    ##
    accessModes:
        - ReadWriteOnce
    ## @param persistence.size PVC Storage Request for etcd data volume
    ##
    size: 1Gi

```

```

    ## @param persistence.selector [object] Selector to match an existing Persistent
    Volume
    ## ref: https://kubernetes.io/docs/concepts/storage/persistent-volumes/#selector
    ##
    selector: {}

## @section Volume Permissions parameters

## Init containers parameters:
## volumePermissions: Change the owner and group of the persistent volume
mountpoint to runAsUser:fsGroup values from the securityContext section.
##
volumePermissions:
    ## @param volumePermissions.enabled Enable init container that changes the owner
    and group of the persistent volume(s) mountpoint to `runAsUser:fsGroup`
    ##
    enabled: false
    ## @param volumePermissions.image.repository Init container volume-permissions
    image name
    ## @param volumePermissions.image.tag Init container volume-permissions image
    tag
    ## @param volumePermissions.image.pullPolicy Init container volume-permissions
    image pull policy
    ##
    image:
        repository: bitnami/os-shell
        tag: 12-debian-12-r21
        pullPolicy: IfNotPresent
    ## Init container' resource requests and limits
    ## ref: https://kubernetes.io/docs/user-guide/compute-resources/
    ## We usually recommend not to specify default resources and to leave this as a
    conscious
    ## choice for the user. This also increases chances charts run on environments
    with little
    ## resources, such as Minikube. If you do want to specify resources, uncomment
    the following
    ## lines, adjust them as necessary, and remove the curly braces after
    'resources:'.
    ## @param volumePermissions.resources.limits [object] Init container volume-
    permissions resource limits
    ## @param volumePermissions.resources.requests [object] Init container volume-
    permissions resource requests
    ##
    resources:
        ## Example:
        ## limits:
        ##     cpu: 500m
        ##     memory: 1Gi
        limits: {}
        requests: {}

## @section Network Policy parameters
## ref: https://kubernetes.io/docs/concepts/services-networking/network-policies/

```

```

##
networkPolicy:
  ## @param networkPolicy.enabled Enable creation of NetworkPolicy resources
  ##
  enabled: false
  ## @param networkPolicy.allowExternal Don't require client label for connections
  ## When set to false, only pods with the correct client label will have network
  ## access to the ports
  ## etcd is listening on. When true, etcd will accept connections from any source
  ## (with the correct destination port).
  ##
  allowExternal: true
  ## @param networkPolicy.extraIngress [array] Add extra ingress rules to the
  NetworkPolicy
  ## e.g:
  ## extraIngress:
  ##   - ports:
  ##     - port: 1234
  ##     from:
  ##       - podSelector:
  ##         - matchLabels:
  ##           - role: frontend
  ##       - podSelector:
  ##         - matchExpressions:
  ##           - key: role
  ##             operator: In
  ##             values:
  ##               - frontend
  ##
  extraIngress: []
  ## @param networkPolicy.extraEgress [array] Add extra ingress rules to the
  NetworkPolicy
  ## e.g:
  ## extraEgress:
  ##   - ports:
  ##     - port: 1234
  ##     to:
  ##       - podSelector:
  ##         - matchLabels:
  ##           - role: frontend
  ##       - podSelector:
  ##         - matchExpressions:
  ##           - key: role
  ##             operator: In
  ##             values:
  ##               - frontend
  ##
  extraEgress: []
  ## @param networkPolicy.ingressNSMatchLabels [object] Labels to match to allow
  ## traffic from other namespaces
  ## @param networkPolicy.ingressNSPodMatchLabels [object] Pod labels to match to
  ## allow traffic from other namespaces
  ##

```

```

    ingressNSMatchLabels: {}
    ingressNSPodMatchLabels: {}

## @section Snapshotting parameters

## Start a new etcd cluster recovering the data from an existing snapshot before
## bootstrapping
##
startFromSnapshot:
    ## @param startFromSnapshot.enabled Initialize new cluster recovering an
    ## existing snapshot
    ##
    enabled: false
    ## @param startFromSnapshot.existingClaim Existing PVC containing the etcd
    ## snapshot
    ##
    existingClaim: ""
    ## @param startFromSnapshot.snapshotFilename Snapshot filename
    ##
    snapshotFilename: ""
## Enable auto disaster recovery by periodically snapshotting the keyspace:
## - It creates a cronjob to periodically snapshotting the keyspace
## - It also creates a ReadWriteMany PVC to store the snapshots
##
disasterRecovery:
    ## @param disasterRecovery.enabled Enable auto disaster recovery by periodically
    ## snapshotting the keyspace
    ##
    enabled: false
    cronjob:
        ## @param disasterRecovery.cronjob.schedule Schedule in Cron format to save
        ## snapshots
        ## See https://en.wikipedia.org/wiki/Cron
        ##
        schedule: "*/30 * * * *"
        ## @param disasterRecovery.cronjob.historyLimit Number of successful finished
        ## jobs to retain
        ##
        historyLimit: 1
        ## @param disasterRecovery.cronjob.snapshotHistoryLimit Number of etcd
        ## snapshots to retain, tagged by date
        ##
        snapshotHistoryLimit: 1
        ## @param disasterRecovery.cronjob.podAnnotations [object] Pod annotations for
        ## cronjob pods
        ## ref: https://kubernetes.io/docs/concepts/overview/working-with-objects/
        ##
        podAnnotations: {}
        ## Configure resource requests and limits for snapshotter containers
        ## ref: https://kubernetes.io/docs/user-guide/compute-resources/
        ## We usually recommend not to specify default resources and to leave this as
        ## a conscious

```

```

    ## choice for the user. This also increases chances charts run on environments
    with little
    ## resources, such as Minikube. If you do want to specify resources, uncomment
    the following
    ## lines, adjust them as necessary, and remove the curly braces after
    'resources:'.
    ## @param disasterRecovery.cronjob.resources.limits [object] Cronjob container
    resource limits
    ## @param disasterRecovery.cronjob.resources.requests [object] Cronjob
    container resource requests
    ##
    resources:
      limits:
        cpu: 500m
        memory: 1Gi
      requests:
        cpu: 1m
        memory: 64Mi
    ## @param disasterRecovery.cronjob.nodeSelector Node labels for cronjob pods
    assignment
    ## Ref: https://kubernetes.io/docs/user-guide/node-selection/
    ##
    nodeSelector: {}
    ## @param disasterRecovery.cronjob.tolerations Tolerations for cronjob pods
    assignment
    ## Ref: https://kubernetes.io/docs/concepts/configuration/taint-and-toleration/
    ##
    tolerations: []

  pvc:
    ## @param disasterRecovery.pvc.existingClaim A manually managed Persistent
    Volume and Claim
    ## If defined, PVC must be created manually before volume will be bound
    ## The value is evaluated as a template, so, for example, the name can depend
    on .Release or .Chart
    ##
    existingClaim: ""
    ## @param disasterRecovery.pvc.size PVC Storage Request
    ##
    size: 1Gi
    ## @param disasterRecovery.pvc.storageClassName Storage Class for snapshots
    volume
    ##
    storageClassName: managed-nfs-storage

  ## @section Service account parameters

  serviceAccount:
    ## @param serviceAccount.create Enable/disable service account creation
    ##
    create: false
    ## @param serviceAccount.name Name of the service account to create or use

```

```

##
name: ""
## @param serviceAccount.automountServiceAccountToken Enable/disable auto
mounting of service account token
## ref: https://kubernetes.io/docs/tasks/configure-pod-container/configure-
service-account/#use-the-default-service-account-to-access-the-api-server
##
automountServiceAccountToken: true
## @param serviceAccount.annotations [object] Additional annotations to be
included on the service account
##
annotations: {}
## @param serviceAccount.labels [object] Additional labels to be included on the
service account
##
labels: {}

## @section Other parameters

## etcd Pod Disruption Budget configuration
## ref: https://kubernetes.io/docs/tasks/run-application/configure-pdb/
##
pdb:
  ## @param pdb.create Enable/disable a Pod Disruption Budget creation
  ##
  create: false
  ## @param pdb.minAvailable Minimum number/percentage of pods that should remain
  scheduled
  ##
  minAvailable: 1
  ## @param pdb.maxUnavailable Maximum number/percentage of pods that may be made
  unavailable
  ##
  maxUnavailable: ""

## @section Security parameters for service mesh
##
security:
  ## @param security.create Enable/disable service mesh security creation
  ##
  create: false
  ## @param security.allowPlaintextClient Switch to disable plaintext client. When
false, client must have tls enabled
  ##
  allowPlaintextClient: false
  ## @param security.allowedClientNamespaces [array] List of namespaces that can
  use a client to talk to the etcd cluster
  ##
  allowedClientNamespaces: []
  ## @param security.allowedMemberNamespaces [array] List of namespaces that can
  have an etcd member in the cluster
  ##
  allowedMemberNamespaces: []

```



```

## @section Routing parameters for service mesh
##
routing:
  ## @param routing.create Enable/disable service mesh gateway creation for etcd
  ##
  create: false
  ## @param routing.enabled Enable/disable service mesh virtual service routing
  creation for etcd
  ##
  enabled: false
  ## ingress gateway ports to use for etcd
  ## @param routing.ingressGatewayPorts.client Client port to use at gateway level
  ## @param routing.ingressGatewayPorts.peer Peer port to use at gateway level
  ##
  ingressGatewayPorts:
    client: 2379
    peer: 2380
  ## @param routing.allowedIpBlocks [array] List of single IP or CIDR that can use
  a client to talk to the etcd cluster or have an etcd member in the cluster
  ##
  allowedIpBlocks: []

## @section Prometheus Rule
##
prometheusRule:
  ## @param prometheusRule.create Specifies whether a PrometheusRule resource
  should be created (alerting rule definitions)
  ##
  # create: false
  ## @param prometheusRule.labels Specify additional labels so the Prometheus
  instance can discover the rules
  ##
  labels: {}

## @section Observability agent
##
obs:
  ## @param obs.enabled Enable/disable observability agent
  ##
  enabled: true
  ## @param obs.image image parameters
  ##
  image:
    ## @param obs.image.repository observability agent image name
    ##
    repository: ""
    ## @param obs.image.tag observability agent image tag
    ##
    tag: ""
    ## @param obs.image.pullPolicy observability agent image pull policy. Defaults
    to 'Always' if image tag is 'latest', else set to 'IfNotPresent'
    ##

```

```

    pullPolicy: IfNotPresent
    ## @param obs.podAnnotations [object] Annotations to add to the pod for
observability (used for prometheus scraping)
    ##
    podAnnotations: {}
    ## @param obs.podLabelsTemplate [object] Labels to add to the pod for
observability (used for pod monitoring) - can contain variables
    ##
    podLabelsTemplate: {}
    ## @param obs.logs log management settings
    ##
    logs:
      ## @param obs.logs.telemetry log telemetry config
      telemetry:
        ## @param obs.logs.telemetry.topic telemetry logs will be sent to this Kafka
topic
        topic: rbbn-otel-agent
      ## @param obs.logs.backendServers log backends
      ##
      backendServers: {}
      ## @param obs.logs.backendServers.elasticsearch elasticsearch backend
      ## Warning: username and password represent the name of the ENV variable
name
      ## that contains the username and password from the secret
      # elasticsearch:
      #   - endpoint: <elasticsearch server address>:443
      #   auth: True
      #   username: ELASTICSEARCH_USER
      #   password: ELASTICSEARCH_PASSWD
      #   index: <filebeat index>
      ## @param obs.logs.backendServers.kafka kafka backend
      ##
      # kafka:
      #   - endpoint: <kafka server address>:<kafka port>
      #   sslCert: KAFKA_CERT
      #   sslKey: KAFKA_KEY
      #   sslCa: KAFKA_CA
      ## @param obs.logs.elasticsearchSecretName Name of secret containing
elasticsearch environment variables
      ##
      elasticsearchSecretName: ""
      ## @param obs.logs.kafkaSecretName Name of secret containing elasticsearch
environment variables
      ##
      kafkaSecretName: ""

      ## @param obs.log.elasticsearchCreds elasticsearch credentials to create
      ##
      elasticsearchCreds:
        create: False
      ## @param obs.log.kafkaCreds kafka credentials to create
      ##
      kafkaCreds:

```

```

        create: False

## @section Common util
##
common-util:
    ## @param common-util.role Role for getting pod logs
    ##
    role:
        ## @param common-util.role.create Specifies whether a Role and RoleBinding
        should be created for the observability components
        create: false
    ## @param global.obs.serviceAccount SA for observability
    ##
    serviceAccount:
        ## @param common-util.serviceAccount.create Specifies whether a service
        account should be created for the observability components
        ##
        create: false
        ## @param common-util.serviceAccount.annotations Annotations to add to the
        service account
        ##
        annotations: {}
        ## @param common-util.serviceAccount.name The name of the service account to
        use.
        ## If not set and create is true, a name is generated using the fullname
        template
        ##
        name: default
    ## @param common-util.logPersistentVolumeStorage Storage request limit for PVC
    ##
    logPersistentVolumeStorage:
        ## @param common-util.logPersistentVolumeStorage.create Specifies whether to
        create a PVC for the storage of log entries
        ##
        create: true
        ## @param common-util.logPersistentVolumeStorage.storageClassName Specify the
        storageClass to be used for the PVC.
        ##
        storageClassName: "managed-nfs-storage"
    persistence:
        ## @param common-util.persistence.annotations Annotations to add to the
        PersistentVolumeClaims
        ##
        annotations:
            volume.beta.kubernetes.io/storage-provisioner: storage.io/nfs
    ## @param common-util.imageCredentials ImagePullSecret creation from credentials
    ##
    imageCredentials:
        ## @param common-util.imageCredentials.create Specifies whether an image
        credentials secret should be created
        ##
        create: true

```

```

## @param common-util.imageCredentials.createPostDelete Specifies whether an
image credentials secret should be created as a post-delete hook
##
createPostDelete: true
## @param common-util.prometheusRule Prometheus alerting rules
##
prometheusRule:
## @param common-util.prometheusRule.create Specifies whether a PrometheusRule
resource should be created
##
create: false

```

Note

Upgrade the additional members similar to the first one. Rebuild each VM, one at a time and allow its replication member to re-synchronize before upgrading the next VM.

For more information, refer to [RAMP CNF etcd Health Check](#).

RAMP CNF etcd Health Check

Use this procedure to check the status of the etcd cluster synchronization and the health of any etcd.

Prerequisite

Ensure you have the necessary permissions and access to the etcd pod.

Start

1. Log on to the etcd pod:

```
oc exec -it <etcd pod name> bash
```

Example output:

```

$ oc exec -it sanetcd1-0-0 bash
kubectl exec [POD] [COMMAND] is DEPRECATED and will be removed in a future
version. Use kubectl exec [POD] -- [COMMAND] instead.
Defaulted container "etcd" out of: etcd, telemetry-agent, network-configurator
(init)

```

2. List the members of the etcd cluster:

```
etcdctl --cacert=/opt/etcd/certs/client/ca.pem --cert=/opt/etcd/certs/client/
cert.pem --key=/opt/etcd/certs/client/key.pem -w table member list
```

Example output:

```
$ etcdctl --cacert=/opt/etcd/certs/client/ca.pem --cert=/opt/etcd/certs/client/cert.pem --key=/opt/etcd/certs/client/key.pem -w table member list
```

ID	STATUS	NAME	PEER ADDRS
CLIENT ADDRS	IS LEARNER		
408921b352a63a76	started	sanetcd3-0	https://10.52.157.74:2380 https://10.52.157.74:2379
4155f7786fa8005e	started	sanetcd2-0	https://10.52.157.73:2380 https://10.52.157.73:2379
fc993425c3830d39	started	sanetcd1-0	https://10.52.157.72:2380 https://10.52.157.72:2379

3. Check the health of the specified etcd endpoints:

```
etcdctl --endpoints=https://<etcd ip>:2379 endpoint health --cert /opt/etcd/certs/server/cert.pem --key /opt/etcd/certs/server/key.pem --cacert /opt/etcd/certs/server/ca.pem -w table
```

Example output:

```
$ etcdctl --endpoints=https://10.52.157.74:2379,https://10.52.157.73:2379,https://10.52.157.72:2379 endpoint health --cert /opt/etcd/certs/server/cert.pem --key /opt/etcd/certs/server/key.pem --cacert /opt/etcd/certs/server/ca.pem -w table
```

ENDPOINT	HEALTH	TOOK	ERROR
https://10.52.157.73:2379	true	7.155783ms	
https://10.52.157.74:2379	true	7.617842ms	
https://10.52.157.72:2379	true	7.595513ms	

Verify that the response confirms all members have a Health status of "true."

Health Check etcd

You can check the status of etcd cluster synchronization and health of any node.

Prerequisites

- The etcd is up and running.

Health Check on etcd

1. Log on as `root` user.
2. Health check the cluster state:

```
root@services3 ~]# etcdStatus.py
```

Example Output:

Name	ID	Endpoint	Leader	Healthy
services1	64386b664d63723b	http://172.29.86.21:2379	false	true
services2	81dcb39d0b4f7142	http://172.29.86.81:2379	true	true
services3	c88e907d0579400a	http://172.29.86.69:2379	false	true

Verify the response identifies one of the members as the Leader, and that all members have a Healthy status of "true".

Rolling Back RAMP CNF

Use the following procedure to roll back an upgraded standalone instance of Ribbon Application Management Platform (RAMP) on Cloud Native Function (CNF).

Prerequisite

Backup files are available. For more information, refer to [Take a Backup of RAMP for Daily Maintenance](#).

Start

1. Uninstall the RAMP deployment and delete the Persistent Volume Claim (PVC). For more information, refer to [Uninstalling RAMP CNF](#).
2. To instantiate RAMP in the previous version, refer to [Installing RAMP CNF](#).
3. To check the status of the RAMP, refer to [Check RAMP Status](#).
4. To restore RAMP, refer to [Restore from Backup on RAMP Standalone](#).

Note

If you need to downgrade RAMP, you must reboot the registered devices to ensure the passwords are synchronized. The reboot is necessary because the older version of RAMP will not have the passwords generated after an upgrade.

Uninstalling RAMP CNF

Related articles:

- [RAMP CNF - Uninstall Using Git](#)
- [RAMP CNF - Uninstall Using Helm Commands](#)
- [RAMP CNF - Delete PVCs](#)

This section provides procedures to uninstall Ribbon Application Management Platform (RAMP) Cloud Native Functionality (CNF) using Helm charts or GitOps.

Based on the current type of installation, select the uninstallation procedure:

- To uninstall using Helm charts, refer to [RAMP CNF - Uninstall Using Helm Commands](#).
- To uninstall using Git, refer to [RAMP CNF - Uninstall Using Git](#).

After you uninstall RAMP CNF using one of the above procedures, you must manually delete the Persistent Volume Claim (PVC). For more information, refer to [RAMP CNF - Delete PVCs](#).

RAMP CNF - Uninstall Using Git

In this section:

- [Uninstall RAMP Using Git](#)
- [Delete PVCs](#)

You can uninstall the Ribbon Application Management Platform (RAMP) Cloud Native Function (CNF) using Git. Use this procedure if you installed RAMP CNF using Git.

Uninstall RAMP Using Git

Start

1. Edit the `kustomization.yaml` file to remove the RAMP CNF deployment file name that was initially included during the installation of RAMP CNF using Git:

```
apiVersion: kustomize.config.k8s.io/v1beta1
kind: Kustomization
nameSuffix: -ssequira
```

```
resources:
  - values_ramp.yaml ---> This is the name of the HelmRelease file
```

2. Commit the changes:

```
git commit
```

3. Push the committed changes:

```
git push
```

Once FluxCD reconciles the configurations, the RAMP CNF deployment is uninstalled from the cluster.

Delete PVCs

After you uninstall RAMP CNF, you must delete the Persistent Volume Claim (PVC) manually.

For more information, refer to [RAMP CNF - Delete PVCs](#).

RAMP CNF - Uninstall Using Helm Commands

In this section:

- [Uninstall RAMP Using Helm Commands](#)
- [Delete PVCs](#)

Use this procedure to uninstall Ribbon Application Management Platform (RAMP) Cloud Native Function (CNF) using Helm commands.

Uninstall RAMP Using Helm Commands

Start

1. Use one of the following Helm commands to uninstall RAMP CNF:

```
helm delete <release_name>
```

Or

```
helm uninstall <release_name>
```


Example:

```
[user@cli-blr-1 rbbn-ramp-cnf]$ helm uninstall sanramp
I0524 22:56:54.840923 1294334 request.go:665] Waited for 1.027922681s due to
client-side throttling, not priority and fairness, request: GET:https://api.blr-
ocp1.lab.rbbn.com:6443/apis/security.openshift.io/v1?timeout=32s
release "sanramp" uninstalled
```

Where, `sanramp` is the RAMP to be uninstalled.

Delete PVCs

After you uninstall RAMP CNF, you must delete the Persistent Volume Claim (PVC) manually.

For more information, refer to, [RAMP CNF - Delete PVCs](#).

RAMP CNF - Delete PVCs

Related articles:

- [RAMP CNF - Uninstall Using Git](#)
- [RAMP CNF - Uninstall Using Helm Commands](#)

After you uninstall Ribbon Application Management Platform (RAMP) Cloud Native Function (CNF), you must delete the Persistent Volume Claim (PVC). Use this procedure to delete the PVCs manually.

Start

1. To list the PVCs after uninstalling RAMP, run the following command:

```
oc get pvc
```

Example showing three PVC instances:

```
[user@cli-blr-1 rbbn-ramp-cnf]$ oc get pvc
sanramp-pmstats-pvc-sanramp-rampcnf-0          Bound
pvc-9e1c2df2-0b05-4f0b-804a-99d277553568      20Gi RWX managed-nfs-storage
5d15h
sanramp-ramp-pv-storage-sanramp-rampcnf-0      Bound      pvc-72590636-
f58e-4b3f-9a39-addb9a443709      130Gi RW0  csi-rbd-sc      5d15h
sanramp-rbbn-otel-agent-pvc-sanramp-rampcnf-0  Bound      pvc-4dc334a3-1eeb-4832-
b809-7b964c93b31d      20Gi RWX  managed-nfs-storage      5d15h
[user@cli-blr-1 rbbn-ramp-cnf]$
```

2. Use the following command to delete the PVCs manually:

```
oc delete pvc <pvc name>
```

Example:

```
user@cli-blr-1 rbbn-ramp-cnf]$ oc delete pvc sanramp-rbbn-otel-agent-pvc-sanramp-  
rampcnf-0 sanramp-ramp-pv-storage-sanramp-rampcnf-0 sanramp-pmstats-pvc-sanramp-  
rampcnf-0  
persistentvolumeclaim "sanramp-rbbn-otel-agent-pvc-sanramp-rampcnf-0" deleted  
persistentvolumeclaim "sanramp-ramp-pv-storage-sanramp-rampcnf-0" deleted  
persistentvolumeclaim "sanramp-pmstats-pvc-sanramp-rampcnf-0" deleted  
[suser@cli-blr-1 rbbn-ramp-cnf]$
```

RAMP User Guide

Additional articles:

- [How to Access RAMP](#)
- [Getting Started with the RAMP User Interface](#)
- [Device Management](#)
- [Device Operations](#)
- [Authentication and Authorization](#)
- [License Management](#)
- [Performance Management](#)
- [RAMP System Configuration](#)
- [RAMP Tools](#)
- [Joint Interoperability Test Command](#)
- [Notifications](#)

This guide contains information and procedures for Ribbon Application Management Platform (RAMP) users.

How to Access RAMP

In this section:

- [GUI](#)
- [REST API](#)
- [Command Line Interface](#)
- [Device CLI Through RAMP](#)

Related articles:

- [System Requirements to Access RAMP on a Web Browser](#)
- [Log onto the RAMP GUI](#)
- [Log onto the RAMP CLI](#)

The primary interfaces used to access Ribbon Application Management Platform (RAMP) are the graphical user interface (GUI), REpresentational State Transfer (REST) APIs, and the command line interface (CLI).

GUI

RAMP provides a GUI for easy access to provision, maintain and administer the system from any [supported web browser](#). This is the most frequently used access method.

For more details, refer to [Log onto the RAMP GUI](#).

REST API

RAMP provides REST APIs as an alternative way to accomplish many of the tasks that users perform using the RAMP GUI. Currently, RAMP provides APIs for key functional areas, including Authentication/Authorization, Fault Management, Performance Management, and License Management functions. For more details, refer to [REST API Documentation](#).

Command Line Interface

The RAMP CLI provides access to a command line where you can complete administrative functions such as upgrades, troubleshooting, and script-based configuration tasks from any machine with network access using a secure shell (SSH) client terminal emulator.

For more details, refer to [Log onto the RAMP CLI](#).

Device CLI Through RAMP

The RAMP CLI supports executing commands to configure the devices directly without logging into the device itself. SSH through port 8122 to access the RAMP CLI.

To access your devices through RAMP, refer to [Device Operations](#).

System Requirements to Access RAMP on a Web Browser

In this section:

- [System Requirements](#)
- [Recommended Web Browser Settings](#)

System Requirements

The following table lists the requirements to access the Ribbon Application Management Platform (RAMP) through a web browser.

Operating system	Windows 10
Web browser	• Chrome version 120.0 • Microsoft Edge 121.0 • Mozilla Firefox version 121.0 Note Enable TLS 1.2 in the web browser to access RAMP.
Plug-in	• OpenJDK Versions: OpenJDK 8, OpenJDK 11, OpenJDK 17, and OpenJDK 21 (required to support PSX Manager) • Openjdk distribution: Oracle OpenJDK, Red Hat OpenJDK, Adoptium (formerly AdoptOpenJDK) • OpenWebstart Version: 1.10.1 Note If you do not have the latest Java version, warning messages display when you attempt to access PSX Manager through RAMP.

Recommended Web Browser Settings

Be aware of the following when using the Ribbon Application Management Platform (RAMP) GUI:

- **Browsers** – Using browsers other than those recommended may result in unpredictable behavior.
- **Cache** – Web browsers cache (save) web pages so that they do not have to download the page every time you access the page.
- **Cookies** – You should enable cookies on each client PC. RAMP uses cookies to persist some user settings.

Note

You may have to clear your browser cache and cookies before accessing newly upgraded RAMP software.

- **Popup blockers** – You must disable popup blockers on your system prior to starting RAMP. Failure to disable popup blockers interferes with the proper operation of RAMP.
- **Desktop shortcuts** – Clicking desktop shortcuts and URL links can launch web pages in an active RAMP window.
- **Drag and drop** – Do not drag and drop to create desktop shortcuts to RAMP. Clicking on a shortcut to RAMP causes an error.
- **Fonts** – RAMP works with the default font settings of your browser and system. Increasing the font size or changing fonts from proportional to fixed width fonts may cause display problems.
- **Keyboard shortcuts** – Do not use browser keyboard shortcuts in conjunction with RAMP. They may cause undesirable results.

Log onto the RAMP GUI

Use the following procedure to access the Ribbon Application Management Platform (RAMP) graphical user interface (GUI). Users who authenticate using the local authentication realm or a Lightweight Directory Access Protocol (LDAP) realm use the RAMP-provided login window. If you use Security Assertion Markup Language (SAML) authentication you do not log in using the RAMP login window. Contact your system administrator for details on your login procedure.

Prerequisites

- Your system meets the requirements listed in [System Requirements to Access RAMP on a Web Browser](#).
- You have login credentials authenticated by either the local authentication realm or an LDAP realm and the IP address for the RAMP system.

Start

1. In a web browser address bar, enter the IP address of the RAMP system in the following format:

`https:// <RAMP FQDN or IP address>`

Note that if you are logging into a system that has implemented multi-tenancy, your login address must also include your tenant ID. Obtain the tenant ID from your system administrator and refer to [Configure Multi-Tenancy](#).

2. In the **Username** and **Password** fields, enter your RAMP login credentials.
3. Check the box acknowledging that you agree to the RAMP terms and conditions.
4. Click **Login**.

Log onto the RAMP CLI

In this section:

- [Log on Using a Password](#)
- [Log on Using an SSH Key](#)
- [Switch to the Insight User](#)
- [Switch to the Root User](#)

Use a secure shell (SSH) to log into the Ribbon Application Management Platform (RAMP) command line interface (CLI). The standard port used by the SSH service, port 22, is appropriate to reach RAMP. From the command line, you can enter Unix or RAMP-specific commands to complete tasks such as starting or stopping the system or retrieving status. Use PuTTY or another terminal emulator to connect to the RAMP CLI.

To maintain security, the type of access allowed to the Linux shell differs for the default accounts provided with RAMP.

The following tables summarize the access allowed in both non-cloud and cloud environments:

Account	Environment	Password	SSH Access	Console access	Sudo access
root	cloud	N/A	no	no	yes
	CNF	N/A	no	no	yes
	non-cloud	N/A	no	no	yes
insight	cloud	static (default)	key-based	no	no
	CNF	user-defined	key-based	no	no
	non-cloud	static (default)	password-based	yes	no
admin	cloud	user-defined	key-based	no	yes
	CNF	user-defined	key-based	no	yes
	non-cloud	static (default)	password-based	yes	yes
System	Privileged user (sudo)		Maintenance user		
RAMP	admin		insight		

To perform certain tasks, a user must use SSH with an account with `sudo` access (admin) to access the Linux shell and then use `sudo` to switch to an account (insight) with permission to access various files and commands that might need to be used for troubleshooting the application. Also note that external access to the root account (key-based or password-based, SSH or console) is disabled; therefore, the root account can only

be accessed through `sudo`. Thus, when logged in as the "admin" user, you can switch to the "insight" user or "root" user accounts when necessary. If you must be logged in as either "insight" or "root" to perform a particular procedure, this is noted in the procedure.

Log on Using a Password

Use the following procedure to log on to the RAMP CLI using a password:

Start

1. `ssh` to the RAMP:

```
ssh <RAMP username>@<RAMP IP address>
```

If this is the initial time you are logging in from a particular system, the message similar to the following displays:

Example:

```
The authenticity of host '[<RAMP ID address>] ([<RAMP ID address>])' can't be
established. RSA key fingerprint is <fingerprint>. Are you sure you want to
continue connecting (yes/no)?
```

2. Enter "yes." The following message displays:

```
Warning: Permanently added '<RAMP ID address>' (RSA) to the list of known hosts.
Password authentication Password:
```

3. Enter the password. The following login information and command prompt display:

```
... Date: <date and time> <RAMP username>@<RAMP host name>: ~ ]#
```

Log on Using an SSH Key

Enter the following command:

```
ssh -i <sshkey> <user>@<RAMP IP Address>
```

Switch to the Insight User

Use the following procedure to switch to an `insight` user:

Start

1. Log on as the `admin` user using one of the previous methods:
2. Enter the following command:

```
sudo su - insight
```

Switch to the Root User

Use the following procedure to switch to the `root` user:

Start

1. Log on as an `admin` user using one of the previous methods:
2. Enter the following command:

```
sudo su -
```

Getting Started with the RAMP User Interface

In this section:

- [Dashboard](#)
 - [Resource Group Dashboard](#)
- [Navigation Menu](#)
- [Global Search Service](#)
- [System Menu](#)
 - [Change User Password](#)
- [Table Controls](#)
- [Customize the Logon Banner](#)

The Ribbon Application Management Platform (RAMP) graphical user interface (GUI) is the primary interface for accessing the RAMP services and features. The topics in this section provide a brief introduction to the RAMP GUI.

Dashboard

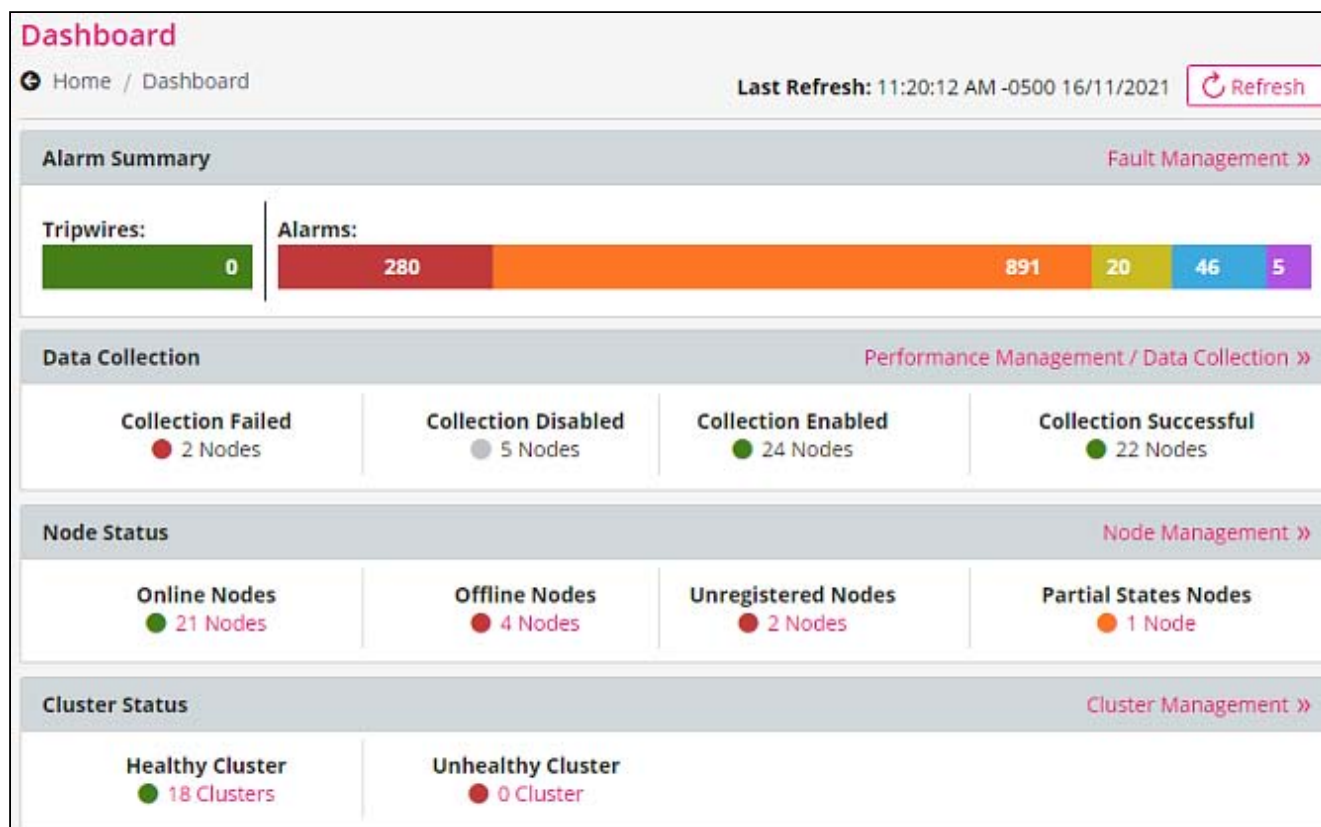
In this section:

- [Alarm Summary](#)
- [Data Collection](#)
- [Node Status](#)
- [Cluster Status](#)

Related articles:

- [Log onto the RAMP GUI](#)
- [Fault Management](#)
- [Performance Management](#)
- [Device Management](#)

The Ribbon Application Management Platform (RAMP) Dashboard provides a concise overview of the health of your managed network. The Dashboard presents data from RAMP's fault management, performance management, and device management services to provide the current status in these key functional areas. The information is color-coded to quickly determine which areas require follow-up actions. You can view the roll-up summary information regarding devices and alarms for a Resource Group in a card format. For more information, refer [Resource Group Dashboard](#).



The following sections provide an overview of the different sections in the dashboard. Note that some areas may not be populated for users who do not have privileges to access the associated service.

Alarm Summary

The Alarm Summary area displays a bar chart representing all the alarms currently raised for the devices registered on RAMP. The relative size and color of each section in the chart are based on the number of alarms in each severity level. If you configure tripwire alarms, customized alarms that trigger based on specific conditions in your network, these are also depicted in the alarm summary. To follow up on alarms in the network, use the **Fault Management (FM)** link to open the **FM Dashboard**.

Refer to [Fault Management](#) for more details on monitoring alarms using RAMP.

Data Collection

The Data Collection area contains a status summary of the data collection aspects of Performance Management (PM). In this summary, the PM service reports how many of the currently registered devices it is configured to retrieve performance metrics from (Collection Enabled). For the devices for which collection is enabled, the Data Collection area also indicates the number of nodes for which the most recent collection interval was successful

(green) and how many failed (red). To follow up on data collection, use the **Performance Management / Data Collection** link to open the **PM Assignment** window to check specific nodes' data collection status.

Refer to [Performance Management](#) for more information on collecting performance metrics data and using RAMP to generate reports or export performance data.

Node Status

The Node Status area summarizes the general status of devices at the node level. In this summary, the Device Management service reports how many nodes are online, offline, unregistered or in a partially registered state. The partial state indicates that the registration process of a node was initiated but the node is not yet fully registered on RAMP. To follow up on devices at the node level, use the **Node Management** link to open the **Node** tab on the **Devices** page that lists information on each node individually.

Cluster Status

The Cluster Status area summarizes the status of devices that are part of a cluster. In this summary, the Device Management service reports how many clusters are considered healthy or unhealthy. If any node in a cluster is offline, then the cluster is considered unhealthy. If all the nodes in a cluster are online, then the cluster is considered healthy. A cluster that currently contains no nodes is still considered healthy. To follow up on devices at the cluster level, use the **Cluster Management** link to open the **Cluster** tab on the **Devices** page that lists information on each cluster individually.

Refer to [Device Management](#) for more information on both node and cluster management using RAMP.

Resource Group Dashboard

The Resource Group screen displays the resource groups in a card-style format. Each card displays resource group information such as total devices, active device count, down device count, alarms, device type, Edge Info, average mos, and EMPath warning.

Note

By default, the resource group dashboard's landing page displays only parent-level resource group cards available to the user.

The parent-level resource group card allows you to drill down into their child resource groups to view children's cards. The parent-level card displays two devices if the parent-level resource group has one device, and the child resource group has one. The same logic applies to other information.

You can filter the resource group cards based on the two drop-down lists.

- **Filter by Criteria:** You can filter by selecting one or more criteria. The criteria supported for this release are down devices, Critical alarm, Major alarm, Minor alarm, Warning alarm, Device types, Low MOS score, Password reset warning, Intermediate alarm and [EMPath Warning](#).
- **Filter by Resource Group:** You can filter by selecting any resource group from the resource groups drop-down list.

Note

The RG dashboard filter criteria depend on the types of devices registered. The parent-level and child-level resource groups appear on the dashboard page if you want to filter the resource group cards based on specific criteria.

The resource group card displays the following information:

Note

The total number of cards on the screen is subject to pagination, with the values 6(by default), 12, and 18.

- **Resource Group name** - You can view the relevant Resource Group details by clicking the link.
 - **MOS Score tab**- The MOS Score tab in the Resource group details page displays the last 24 hours average MOS score in graph format. It is visible only if an EdgeMarc device is present in that resource group and will not be visible for other device types.

Note

While calculating 24-hour average MOS score data, the parent resource group calculates the average MOS score data of the child resource groups as well.

- **Child RG dropdown** - Displays the whole child hierarchy of parent RG. You can select any child RG card from that dropdown to see information about that child RG.
- **Devices** - The total number of devices accessible and their classification as per the number of Active and Down devices.
 - Hover over to see the number of active and inactive devices based on their type and total number of devices.
- **Alarms** - This displays the alarm breakdown based on severity, including **Critical**, **Major**, **Minor**, **Warning**, and **Indeterminate**.
 - Click Alarms to view the FM Dashboard. A popup window will display the alarm details of that specific resource group.
- **Edge Info** - Display edge devices related information such as Avg MOS, PW and EMPATH.

Note

This is applicable for Edge only devices. Any particular EdgeMarc or SBC Edge device should belong to a single resource group. If a device belongs to more than one resource group, the RG Dashboard card (in which the device was last added) becomes the one to represent the Edge Info section corresponding to this device.

- **Avg MOS** - Calculated average MOS value of the last 1 hour of all EdgeMarc devices present in the particular resource group and its children resource groups.
- **PW** - The number of EdgeMarc devices in a resource group and child resource groups with their default password changed randomly.

- **EMPath** - The total number of EdgeMarc and SBC Edge devices connected over HTTPS in a resource group and its child resource groups. A strike out icon next to EMPath indicates that the count pertains to EMPath warnings.

Perform the following to view the child card data:

1. Go to the child drop-down. **Select a Child RG.** All the child resource groups in the hierarchy are displayed.
2. You can traverse to any child resource group and select within that resource at any time.
3. Select a child from the list to display the card with respect to the child card.
4. You can view the information of the Alarm count specifically for the selected RG and child RGs.
5. Click the Alarm header on the RG card. A popup window with the alarm details for that specific resource group is displayed.
The alarm information of both the parent-level and the child-level RGs are displayed.
6. You can filter, paginate, and refresh the alarms.

Note

The alarms are read only.

7. After traversing, if you want to check the RG information of the immediate parent, you can do it through child hierarchy dropdown.
8. Click **Reset** to go back to the topmost parent-level resource group.

Navigation Menu

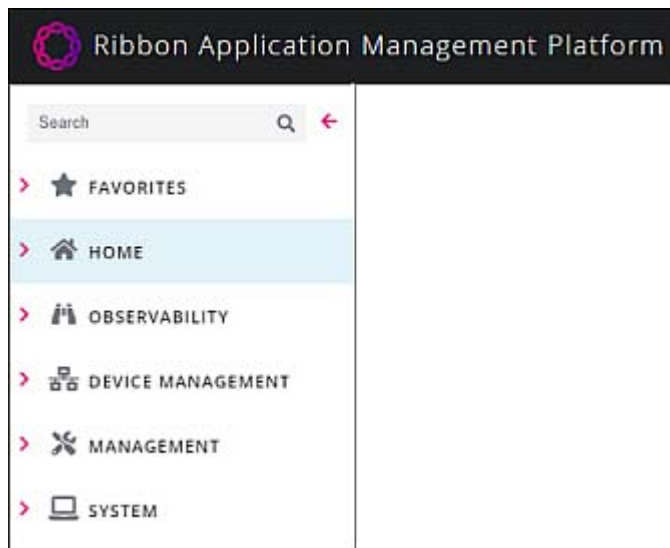
In this section:

- [Search](#)
- [Add Favorites](#)

Related articles:

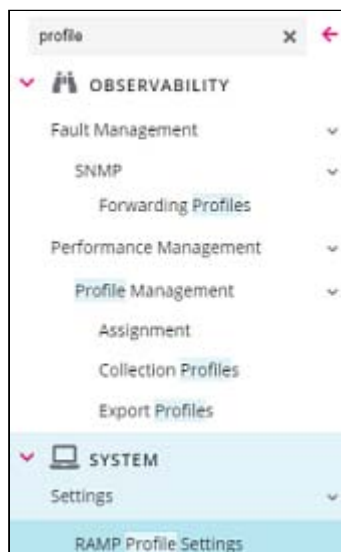
- [Authentication and Authorization](#)
- [Configure Local Authentication](#)

The main Ribbon Application Management Platform (RAMP) navigation menu appears on the left side of the interface. Windows within the interface are arranged hierarchically under different headings. Use the arrows to expand and collapse the categories.



Search

Use the **Search** field to locate specific menu items based on the name. As you enter characters, RAMP filters the list of titles to include those that match. In the following example, the search term is "profile." The RAMP includes any parent or child windows for the matching title or titles to provide context. Clear the **Search** field to restore the full menu.



RAMP is configured with a set of keywords that you can enter as a search term to return a list of related pages.

For example, if you want to enable or disable notifications, the preset keyword is email and mail. When you search for mail or email, RAMP lists the Notifications page.

The table lists the configured keywords per page in the order in which the pages appear in the sidebar menu.

Use these keywords to search for items:

Sidebar Pages	Keywords
Home -> Dashboard	chart, graph

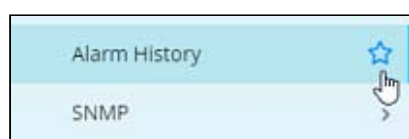
Sidebar Pages	Keywords
Observability -> Fault Management -> FM Dashboard	fmdata, faults
Observability -> Fault Management -> Alarm History	trap history, trap list, trap count, alarm count, alarm list
Observability -> Fault Management -> SNMP -> Forwarding Profiles	forward traps, snmp
Observability -> Fault Management -> SNMP -> Reclassification Rules	Alarm rules, customize alarms
Observability -> Fault Management -> SNMP -> OSS Trap Resync	resync
Observability -> Fault Management -> Notifications	email, mail
Observability -> Fault Management -> Administration	FM Settings
Observability -> Performance Management -> Profile Management -> Assignment	PM
Observability -> Performance Management -> Profile Management -> Collection Profiles	stats collection
Observability -> Performance Management -> Profile Management -> Export Profiles	stats export
Observability -> Performance Management -> Administration	PM settings
Device Management -> Devices	node list, node table, device list, device table
Management -> License Management -> Feature Licenses	LM, license list, license table
Management -> License Management -> Manual Reports	license reports, LM reports
Management -> License Management -> Post-Paid Reports	node level reports, network level reports, license reports, LM reports
Management -> License Management -> Administration	LM settings, license settings

Sidebar Pages	Keywords
Management -> Authentication & Authorization -> Users	profiles, AA, user list
Management -> Authentication & Authorization -> User Groups	group of users, group list
Management -> Authentication & Authorization -> Roles	privilege, resources list, permission
Management -> Authentication & Authorization -> Security Realms	password rules, password complexity
Management -> Authentication & Authorization -> Activity	task, task list, User Activity, AA Activity
Management -> Authentication & Authorization -> Administration	AA settings
Management -> User Sessions	Active Session, https session, telnet session, session count, ssh session, http session
Management -> Session Expiry	terminate, timeout
System -> Application Config	component settings, application settings
System -> Troubleshooting -> System Activity	Live Log, Live System Activity Log, Live System Activity
System -> Interfaces -> Logs	remote server, Syslog server
System -> Interfaces -> Device REST Credentials	REST username, REST password
System -> Settings -> RAMP Profile Settings	Feature Settings, Node Settings, Display settings
System -> Settings -> Database Configuration	Connection Timeout, Connections
System -> Settings -> Logon Banner	Warning message, Login message, message
System -> Settings -> Managed Device Association	associate devices, disassociate devices, link devices
System -> Settings -> PSX Policy Server -> PSX Manager Versions	PSX version

Sidebar Pages	Keywords
System -> Settings -> PSX Policy Server -> Trace Destinations	PSX Trace destination

Add Favorites

For windows you access often, use the **Favorites** option to include the window in a list of shortcuts. To add a title to your favorites list, hover your cursor to the right of a page title until a star appears. Click on the star to add the title under **Favorites**. Favorites are stored in a browser cookie, so your Favorites list is available when you log into RAMP again using the same browser.



To remove a favorite from the list, click the delete icon to the right of the entry in the **Favorites** list.



Global Search Service

In this section:

- [Global Search Service](#)
- [Global Search Service for Backup](#)
- [Global Search Service for Restore](#)
- [Global Search Service for Upgrade](#)

The Ribbon Application Management Platform (RAMP) provides a Global Search Service (GSS) to search components and devices available on the RAMP Graphical User Interface (GUI). The GSS functionality is available after manually installing an optional microservice GSS using the script

`global_search_service_config` after installing the RAMP. Once the microservice runs, the RAMP publishes a confirmation message over the `kafka` topic, `service.availability_status`. The other

microservices consume the `kafka` message and then register themselves with the GSS by sending the register request, enabling access to the GSS to display the search results.

Global Search Service

Prerequisite

Install the `global_search_service_config` script:

```
/opt/global_search_service_config add
```

Perform the following procedure to search using the GSS:

Start

1. Log on to the RAMP GUI.
2. Click the magnifying glass icon at the top right corner of the RAMP GUI to expand to the text field.
3. Type the text you want to search for on the RAMP GUI and press **Enter**. The **Global Search** window displays.
 - a. If the text is not present on the RAMP GUI, it displays a message stating **No records found**.
 - b. If the text is present on the RAMP GUI, the **Global Search** window displays:

Parameter	Description
Search Keyword	Displays the search field with the original keyword
Search Modules	Displays all the searched components on the RAMP GUI, matching the highlighted Search Keyword . Select a module to display the associated objects in the table.
Table	Objects are listed for the selected highlighted Search Module .

- c. If multiple modules are displayed, select each module to switch between the various modules to view the respective search results in the table.
- d. Click ">" to expand each component in the table to view more details.
- e. Click the hyperlink on each component in the table to redirect to its component list page. You can then access the components and perform desired actions on these components.
- f. Click the back arrow at the top left corner of the page to return to the search results window.

Global Search Service for Backup

In the case of a RAMP backup, if the GSS is installed then a backup of the `gssdb` (Global Search Service Database) is taken. The backup is initiated by the script: `global_search_service_config` by providing `backup` as argument.

Global Search Service for Restore

While restoring a RAMP, if the GSS backup is available and the GSS is installed on the RAMP system to restore, only the GSS is restored. Restore is initiated by the script: `global_search_service_config` by providing `restore` as argument.

Global Search Service for Upgrade

In the case of a RAMP upgrade, if the GSS is installed on the RAMP system to upgrade, only the search service gets upgraded. Upgrade is initiated by the script: `global_search_service_config` by providing `upgrade` as argument.

System Menu

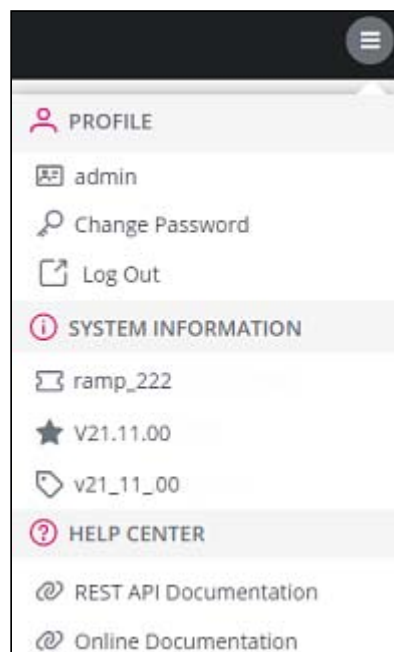
In this section:

- [Profile](#)
- [System Information](#)
- [Help Center](#)

Related articles:

- [Change User Password](#)

Access the Ribbon Application Management Platform (RAMP) system menu by clicking on the icon in the top-right corner of the RAMP graphical user interface (GUI). Its options are divided into three areas.



Profile

The Profile area identifies which user account is currently logged into RAMP and it provides a **Log Out** option you click on to log out of the application.

From the Profile area you can access the interface to change the password for the current account. This option is specific to those logging into RAMP through the local authentication realm and does not apply to those who log in using an external authentication method such as LDAP or SAML. Refer to [Change User Password](#) for the procedure.

System Information

The System Information area identifies the system name for the RAMP system to which you are logged in and the current software version number. These system details may be needed when troubleshooting or planning an upgrade.

Help Center

The Help Center contains a link to online documentation for the RAMP REST APIs. This documentation is the primary source for detailed documentation on the REST APIs. Refer to [REST API Documentation](#) for general information on using the RAMP REST APIs.

The Help Center also provides a link to online documentation for the RAMP application.

Change User Password

Related articles:

- [Authentication and Authorization](#)
- [Configure Local Authentication](#)

Use the **Change Password** window to change your login password for Ribbon Application Management Platform (RAMP). This procedure applies only to changing the password for users who authenticate using the local authentication realm and does not apply to users who authenticate using an external realm such as LDAP or SAML.

Start

1. Log on to RAMP GUI using your current password.
2. Click the system menu icon menu bar in the upper-right side of the GUI.
3. Select **Change Password** to open the **Change Password** window.
4. (Optional) Check the **Show Password Rules** option to see a list of requirements for a new password.
5. In **Current Password**, enter your current password. Note that in any of the password entry fields, you can click the  icon to see what you enter in clear text.
6. In **New Password**, enter the new password.
7. In **Confirm New Password**, enter the same new password again.
8. Click **Change Password**.

Table Controls

In this section:

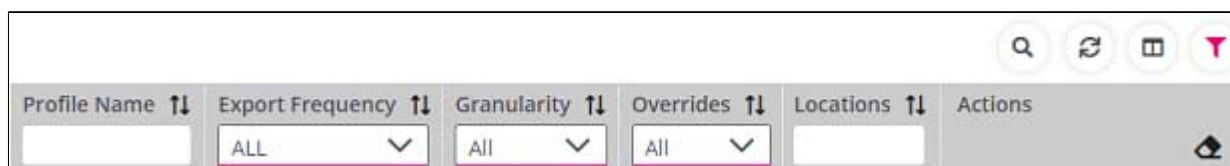
- [Filter Contents](#)
- [Search Contents](#)
- [Select Columns](#)
- [Sort Contents](#)
- [Refresh the Table](#)
- [Actions](#)
- [Bulk Actions Menu](#)

The Ribbon Application Management Platform (RAMP) interface uses tables to present many types of data. In many cases, RAMP tables contain a large amount of data. To help you work with table data effectively, RAMP provides a number of controls that enable you to filter and sort the data in the table and work with the listed objects.

The following sections describe the table controls available in RAMP. Note that the exact set of controls available for each table depends on the contents of the table.

Filter Contents

Click on the funnel icon () to open a "filter row" area at the top of a table. A row of entry fields and selection lists open under the column headings in the current table. You can use these fields to filter the contents of the table. The following is an example filter row for the Export Profile table. In the fields and list provided, enter or select values for a column to include only rows that match the selected value. RAMP filters the contents of the table as you make each selection. You can select a filter value in more than one column to continue refining the contents of the table.



To remove filtering from a table use the clear column filters icon () that appears on the far-right side of the filter row.

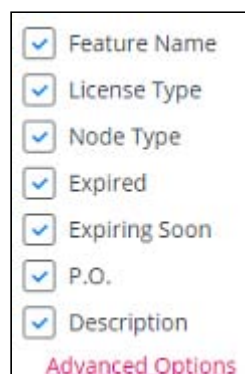
Search Contents

Some tables provide a search option to filter the contents of a table based on a specified search term. When you enter a search term, only those data rows that include the search term appear in the table. The previous image shows an example of a search field. Clear the search field to remove the filtering based on the search term.

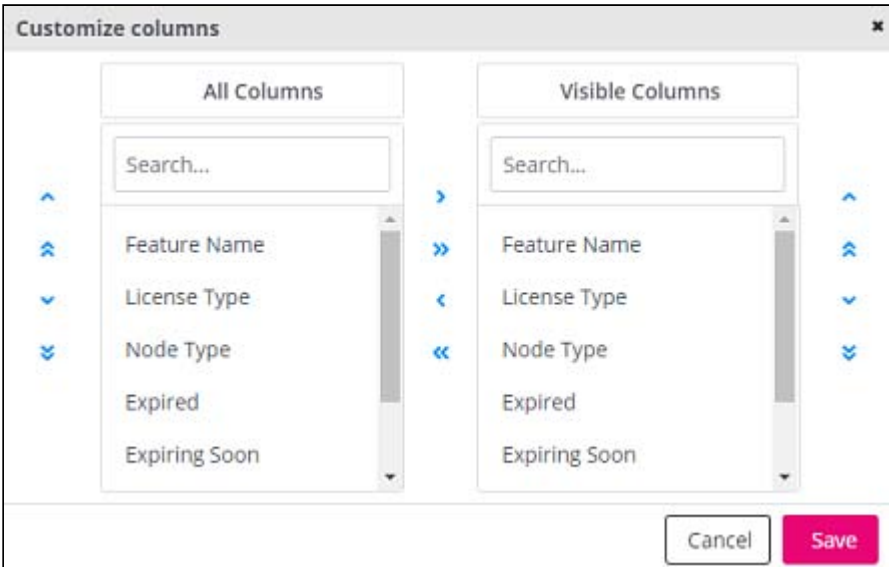
Note that you can use the filter and search functions together.

Select Columns

Click on the show/hide columns icon () to open a list of all the available columns for that table. Place a check mark next to the columns you want to appear in the table and uncheck any columns that you do not want. If a column is mandatory for the table the heading is listed, but cannot be deselected. The following figures show both styles of show/hide column lists.



If the show/hide column list includes an **Advanced Options** link, you can open the **Customize columns** window to both select the columns to make visible, and arrange the order of the columns using the up/down arrows.



Sort Contents

RAMP allows you to sort tables based on most columns in a table. Sort icons appear adjacent to columns that can be used to sort the table. Click the up and down arrows (↕) adjacent to a column name to sort the table based on that column.

Refresh the Table

Click the Refresh icon (↻) to update the table with current values.

Actions

For configuration objects within tables RAMP provides **Actions** icons to perform common operations on a specific object in the table. For example, icons for actions such as copy and delete appear under **Actions** where appropriate. The icons available differ based on the specific type of object and may be disabled if an action cannot be applied to a specific instance. For example, deleting may be disabled for a default profile object, but allowed for user-defined profiles. Operations you select under **Actions** apply only to the object in the selected row.

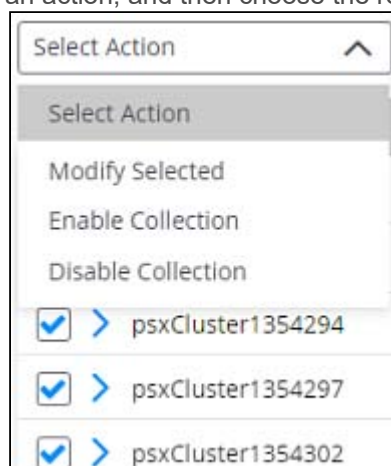
Profile Name ↕	Export Frequency ↕	Granularity ↕	Overrides ↕	Locations ↕	Actions
Default Profile For ...	Every 5 minutes	All	0	1	Copy
SampleExportProfile	Every 5 minutes	All	0	1	

6 - 7 of 7 << < 1 2 > >> 5 ▾

Bulk Actions Menu

In contrast to individual **Actions** icons, RAMP allows you to perform bulk actions on objects in some tables. Use a Bulk Actions option to apply the same operation to multiple objects in the table at once. Bulk Actions menus appear at the top-left of a table. Select the checkboxes next to the table elements on which you want to perform

an action, and then choose the required action from the **Select Action** menu.



Customize the Logon Banner

Use the **Logon Banner** window to add customized text to the Ribbon Application Management Platform (RAMP) login window. For example, you might use a custom message to alert users to upcoming system maintenance or changes to rules for those using the system. Users logging into RAMP will see the message on the RAMP login window.

Prerequisite

You have Super User [privileges](#) for the **Insight Administration** resource within **Core Resources**.

Start

1. Log onto the RAMP GUI.
2. Navigate to **System > Settings > Logon Banner**
3. Enter the message you want to display on the logon page and the banner content for JITC authentication.
4. Click **Apply**.

Device Management

In this section:

- [Registering Devices on RAMP](#)
- [Manage Registered Nodes](#)
- [Manage Clusters](#)
- [Launching Device GUIs from RAMP](#)
- [Work with Resource Groups](#)
- [Work with Inventory Reports](#)
- [Modify Managed Device Association](#)
- [Configure Device Management Administration Options](#)
- [Firmware Repositories](#)

The Ribbon Application Management Platform (RAMP) Device Management services provide a range of software and network management functions for both hardware-based and virtualized Ribbon devices. The

Device Management services facilitate device configuration, managing nodes and clusters, organizing nodes and clusters into resource groups, inventory management, and software management.

The prerequisite for managing any device is registration with RAMP, which bring the device into the managed network. The following sections provide a brief overview of device registration on RAMP.

Device Registration on RAMP

RAMP supports manual, dynamic, and automatic registration for managed devices. Refer to the documentation for a specific device to determine which modes it supports in specific deployment environments.

Take the device type and environment into consideration before initiating the registration process:

- Hardware/physical devices support only manual registration.
- Cloud devices configured in clusters support only dynamic registration.
- SBC and PSX devices on KVM/VMware support both manual and dynamic registration.
- SBC Edge devices automatically register on RAMP, without clusters, by configuring the RAMP IP address on the Edge device.

Manual Registration

Manual registration of a device on RAMP can be initiated only after installing the device and when it is up and running.

The device is registered on RAMP using the IP address of the device. Each type of device has its own registration parameters presented through the RAMP GUI. Depending on the device type and your network, RAMP requires you to provide different types of credentials and configuration parameters.

To register devices manually, refer to [Manually Register Devices on RAMP](#).

Dynamic Registration with Clusters

RAMP supports managing groups of interrelated devices by placing them into device clusters on RAMP. Prior to instantiating the devices, you must create a cluster with unique cluster ID on RAMP. This configuration includes a cluster ID among its parameters. During instantiation, you supply the device with the RAMP IP address or FQDN and the cluster ID so that the device locates its appropriate cluster configuration on RAMP. The device then initiates dynamic registration with RAMP, as part of the cluster, when it is deployed. Refer to [Create Clusters for Devices that Dynamically Register with RAMP](#) for more information.

SBC and PSX devices support the concept of service discovery for determining how to access RAMP. The service discovery capability enables you to specify an FQDN for RAMP instead of a static IP address. If RAMP is identified with an FQDN, when the RAMP IP address changes, a DNS administrator can simply update the IP address associated with the FQDN in DNS records, rather than reconfiguring the individual devices. The SBC/PSX devices automatically detect the updated RAMP IP address.

For more information on SBC/SLB service discovery, refer to [Service Discovery for Trap Target Destinations and RAMP Registration](#).

SBC Edge Automatic Registration

RAMP supports automatically registering Edge devices without creating clusters. For more information, refer to [Register an SBC Edge Device](#).

Registering Devices on RAMP

In this section:

- [Manually Register Devices on RAMP](#)
 - [Register an AS Device](#)
 - [Register a C3 or G9EMS Devices](#)
 - [Register a C20 Device](#)
 - [Register a DELL Device](#)
 - [Register a DSC Device](#)
 - [Register a DSI Device](#)
 - [Register a G5 Device](#)
 - [Register a G6MM Device](#)
 - [Register a GMS Device](#)
 - [Register a GSX Device](#)
 - [Register an IDH Device](#)
 - [Register an L2MGR Device](#)
 - [Register a PSX Device](#)
 - [Register an SBC Core Device](#)
 - [Register an SGX Device](#)
 - [Register an SLB Device](#)
 - [Register an STI Device](#)
- [Automatically Register Devices on RAMP](#)
 - [Register C20 Devices](#)
 - [Register an Edge 8000 Device](#)
 - [Register an SBC Edge Device](#)
 - [Register an EdgeMarc Device](#)
- [Create Clusters for Devices that Dynamically Register with RAMP](#)
 - [Create SBC Clusters](#)
 - [Create SLB Clusters](#)
 - [Create PSX Clusters](#)
- [Edit RAMP Device Registration](#)

Registering your devices on Ribbon Application Management Platform (RAMP) is the first step for managing the devices with RAMP. Depending on the type of device and whether registration is manual or dynamic, the registration process differs. Refer to the topics for a specific device type and mode of registration for the options and procedures.

After a device is registered and discovered by RAMP, the two devices communicate with each other. The managed devices can send fault, performance, and inventory information. RAMP polls the devices and services on the devices. Polling is to check if a device is active or inactive. If the device is inactive an alarm is raised. You can configure the frequency of polling. For information on polling, refer to [Application Configuration](#).

RAMP supports manual, dynamic, and automatic registration for managed devices:

In Dynamic Registration, the RAMP cluster ID and the REST credentials are provided in the user data while instantiating the device. The device registers dynamically to the given cluster in RAMP as part of the device bootup sequence. This device sends the `registernode`, the credentials and the `instanceup` REST requests to complete the registration.

In an Automatic Registration, the RAMP connection parameters are configured on the device through the device GUI or CLI to register the device automatically in RAMP using register REST API. The same REST API is used in RAMP GUI for manual registration.

Managed Devices	Manually Registered	Automatically Registered	Dynamically Registered
AS	Yes	No	No
C3 G9EMS	Yes	No	No
C20	Yes	Yes	No
DELL	Yes	No	No
DSC	Yes	No	No
DSI	Yes	No	No
EdgeMarc	No	Yes	No
G5	Yes	No	No
G6MM	Yes	No	No
GMS	Yes	No	No
GSX	Yes	No	No
IDH	Yes	No	No
L2MGR	Yes	No	No
PSX	Yes: Pre-PSX 15.x	No	Yes
SBC Core	Yes	No	Yes

Managed Devices	Manually Registered	Automatically Registered	Dynamically Registered
SGX	Yes	No	No
SLB	Yes	No	Yes
STI	Yes	No	No
Edge 8000	No	Yes	No
SBC Edge	No	Yes	No

For information on registration concepts, refer to [Device Management](#).

For the PSX, Manual Registration applies for PSX 14.x and earlier versions on KVM/VMWare. Dynamic Registration is required for PSX 15.x and later and for all releases deployed in Public/Private Cloud.

For the SBC Core and SLB, Manual Registration applies for nodes deployed on KVM/VMWare. Dynamic Registration is required for instances deployed in Public/Private Cloud.

Manually Register Devices on RAMP

In this section:

- [Register an AS Device](#)
- [Register a C3 or G9EMS Devices](#)
- [Register a C20 Device](#)
- [Register a DELL Device](#)
- [Register a DSC Device](#)
- [Register a DSI Device](#)
- [Register a G5 Device](#)
- [Register a G6MM Device](#)
- [Register a GMS Device](#)
- [Register a GSX Device](#)
- [Register an IDH Device](#)
- [Register an L2MGR Device](#)
- [Register a PSX Device](#)
- [Register an SBC Core Device](#)
- [Register an SGX Device](#)
- [Register an SLB Device](#)
- [Register an STI Device](#)

The Ribbon Application Management Platform (RAMP) supports manually registering devices. Procedures for manually registering different types of devices on RAMP are provided on the pages in this section.

Register an AS Device

Use this procedure to manually register an Application Server (AS) on the Ribbon Application Management Platform (RAMP). This involves configuring the System Manager (SM) and Fault Performance Manager (FPM) Application Server Network Elements (NEs) for AS devices on RAMP.

Prerequisites

- The SM or FPM device is up and running.
- The RAMP is configured as an SNMP Manager on the AS (through the SM GUI).
- The RAMP SNMP Manager is assigned to the SM or the FPM as an Alarm Processing SNMP Manager.
- The **Enable Trap Resync** checkbox for the supported devices is selected from **Observability**, **Fault Management**, **Administration**, and **Process** GUI.

Start

Perform the following procedure to register an AS:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. For **Device**, select "Node."
5. For **Type**, select "AS."
6. Configure additional AS registration parameters using the following table and click **Save**.

AS Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • Root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the AS device to an existing resource group. • Root • <any other existing resource group>
Device	N/A	Select Node to register an AS instance. • Node

Parameter	Length/Range	Description
Type	N/A	Select AS as the device type. • AS • C20 • C3 G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • L2MGR • PSX • RAMP • SBC Core • SGX • SLB
Node Information		
Name	1 to 64 characters Do not use special characters like ^[^\<>.:;,+=*?"'<> !@#\$\$%^&() `{}]*\$	Provide a unique name for the node.
REST URL	N/A	Enter the secure REST URL in the form https://<SM-Service-IP>:12121 You must enter the SM Service IP for both SM and FPM devices.
Node IP		
Primary IP	IPv4 address format	Enter the active IP address of the SM or the FPM.
Secondary IP	N/A	Not applicable to AS devices.
Interfaces		
REST		

Parameter	Length/Range	Description
Username	N/A	Enter the REST API user name. You must create a unique dedicated OMI user on the AS to be used by RAMP.
Password	N/A	Enter the REST API password.
SNMP Configuration Rediscover the devices after updating the SNMP configuration.		
Note Specify the SNMP configuration. For more information, refer to SNMP Configuration.		
SNMP Read Community	1 to 72 alphanumeric characters	Applicable only for SNMP V2c (not SNMP v3) This is the community string for traps and reachability. If the community string is incorrect, AS ignores the reachability requests and does not respond. If you change the value in RAMP, update this value on the AS. For more information, refer to SNMP Configuration
Port	N/A	The SNMP port number used for the device. The default port number is "161".

Parameter	Length/Range	Description
SNMPv3 Security Level	N/A	The parameter is applicable only for SNMPv3. If you change the value in RAMP, update this value on the AS. Select the type of security model to apply to SNMP connections: • None (default) – no security. • AuthPriv – authentication is required, and messages are encrypted. • AuthNoPriv – connections using this model must authenticate, but the messages are sent without encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private.
SNMPv3 User	5 to 32 alphanumeric characters	This parameter is applicable only if the Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv Enter the SNMPv3 user's username for authentication. If you change the value in RAMP, update this value on the AS.
SNMPv3 Authentication Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. Select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol to enable private interactions over secure channels. If you change the value in RAMP, update this value on the AS. • SHA • MD5 (default)

Parameter	Length/Range	Description
SNMPv3 Auth Passphrase	8 to 32 characters	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. This is the SNMPv3 authorization password. If you change the value in RAMP, update this value on the AS. The default value is "admin123".
SNMPv3 Privacy Protocol		This parameter is applicable only if the Security Level is set to AuthPriv. Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. If you change the value in RAMP, update this value on the AS. • AES (default) • DES
SNMPv3 Priv Passphrase	8 to 32 characters	This parameter is applicable only if the Security Level is set to AuthPriv. This is the SNMPv3 privacy password. If you change the value in RAMP, update this value on the AS. The default value is "admin123".
Management Client		
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.

Parameter	Length/Range	Description
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP

SNMPv3 Security Levels

SNMPv3 Security Level	SNMPv3 User	SNMPv3 Authentication Protocol	SNMPv3 Authentication Key	SNMPv3 Privacy Protocol	SNMPv3 Privacy Key
None	-	-	-	-	-
NoAuthNoPriv	✓	-	-	-	-
AuthNoPriv	✓	✓	✓	-	-
Authpriv	✓	✓	✓	✓	✓

Register a C3 or G9EMS Devices

You can manually register C3 or G9EMS devices on Ribbon Application Management Platform (RAMP). To configure C3 or G9EMS devices on RAMP, the RAMP IP address must be configured on the C3 or G9EMS system parameters section. For more information, refer to [G9 Converged Gateway Documentation](#).

Prerequisites

- The C3 or G9EMS devices are up and running.
- RAMP IP address is configured in the C3 or G9EMS system parameters section.
- [Super User](#) privileges for Insight Administration under Core Resources.
- **Devices** and **Resource Groups** [privileges](#) under Device Management.

Start

Perform the following procedure to register a C3 or G9EMS devices:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **C3** or **G9EMS**.
5. Configure the C3 or G9EMS registration parameters using the following table and click **Save**.

C3 or G9EMS Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the C3 or G9EMS device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register a C3 or G9EMS instance. • Node

Parameter	Length/Range	Description
Type	N/A	Select C3 or G9EMS as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters.	Provide a unique name for the node. Do not use special characters such as: ^[^\<>.:;,+=*?"'<> !@#\$\$%^&() `{}]*\$.
Node IP		
Primary IP	N/A	Enter the default or primary IP address.
Secondary IP	N/A	Enter the default or secondary IP address.
Interfaces		
REST		
Username	N/A	Enter the REST API user name. The default user name is "admin".
Password	N/A	Enter the REST API password. The default password is "admin".

Parameter	Length/Range	Description
SNMP Configuration		
Rediscover the devices after updating the SNMP configuration. Refer to Discover Nodes for details.		
SNMP Read Community	1 to 72 alphanumeric characters.	This is the community string for traps, resync, and reachability. If the community string is incorrect, C3 or G9EMS ignores the request and does not respond. If you change the value in RAMP, update this value on C3 or G9EMS . The default value is "public".
Port	N/A	The SNMP port number used for the device. The default port number is "161".
SNMPv3 Security Level	N/A	Note SNMPv3 Security Levels are currently not supported for C3 or G9EMS. The parameter is applicable only for SNMPv3. Select the type of security model to apply to SNMP connections: • None (Default) – no security. • AuthPriv– authentication is required, and messages are encrypted. • AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private.

Parameter	Length/Range	Description
SNMPv3 User	5 to 32 alphanumeric characters.	Note This parameter is applicable only if the Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv Enter the username of the SNMPv3 user for authentication.
SNMPv3 Authentication Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. To enable private interactions over secure channels, select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol. • SHA (default) • MD5
SNMPv3 Auth Passphrase	8 to 32 characters.	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. This is the SNMPv3 authorization password. The default value is "admin123".
SNMPv3 Privacy Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv. Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. • AES (default) • DES

Parameter	Length/Range	Description
SNMPv3 Priv Passphrase	8 to 32 characters.	This parameter is applicable only if the Security Level is set to AuthPriv. This is the SNMPv3 privacy password. The default value is "admin123".
Management Client		
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		

Parameter	Length/Range	Description
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP • REST (default)

SNMPv3 Security Levels

SNMPv3 Security Level	SNMPv3 User	SNMPv3 Authentication Protocol	SNMPv3 Authentication Key	SNMPv3 Privacy Protocol	SNMPv3 Privacy Key
None	-	-	-	-	-
NoAuthNoPriv	✓	-	-	-	-
AuthNoPriv	✓	✓	✓	-	-
Authpriv	✓	✓	✓	✓	✓

Register a C20 Device

You can manually register C20 Call Session Controller (C20) devices deployed on KVM on the Ribbon Application Management Platform (RAMP). The first step is to configure the device through the CLI on the C20. Refer to [C20 Manual Registration](#) and then register the device on RAMP through the RAMP GUI.

Prerequisites

- The C20 device is up and running.
- The C20 is already configured through the C20 CLI for RAMP registration.
- [Super User](#) privileges for Insight Administration under Core Resources.
- Devices and Resource Groups [privileges](#) under Device Management.

Start

Perform the following procedure to register a C20 device:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **C20**.
5. Configure the C20 registration parameters using the following table and click **Save**.

C20 Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the C20 device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register a C20 instance. • Node
Type	N/A	Select C20 as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		

Parameter	Length/Range	Description
Name	1 to 64 characters.	Provide a unique name for the node. Do not use special characters such as: ^[\^<>.:;,+=*?\\"<> !@#\$\$%^&() `{}]*\$.
Node IP		
Primary IP	N/A	Enter the default or primary IP address.
Secondary IP	N/A	Enter the default or secondary IP address.
FQDN	N/A	Enter the Fully Qualified Domain Name (FQDN).
Interfaces		
REST		
Username	N/A	Enter the REST API user name. The default user name is "admin".
Password	N/A	Enter the REST API password. The default password is "admin".
SNMP Configuration		
Rediscover the devices after updating the SNMP configuration. Refer to Discover Nodes for details.		
SNMP Read Community	1 to 72 alphanumeric characters.	This is the community string for traps, resync, and reachability. If the community string is incorrect, C20 ignores the request and does not respond. If you change the value in RAMP, update this value on C20. The default value is "hefj6483xhie".
Port	N/A	The SNMP port number used for the device. The default port number is "161".

Parameter	Length/Range	Description
SNMPv3 Security Level	N/A	The parameter is applicable only for SNMPv3. Select the type of security model to apply to SNMP connections: • None (Default) – no security. • AuthPriv – authentication is required, and messages are encrypted. • AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private.
SNMPv3 User	5 to 32 alphanumeric characters.	Note This parameter is applicable only if the Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv Enter the username of the SNMPv3 user for authentication.
SNMPv3 Authentication Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. To enable private interactions over secure channels, select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol. • SHA (default) • MD5

Parameter	Length/Range	Description
SNMPv3 Auth Passphrase	8 to 32 characters.	This parameter is applicable only if Security Level is set to AuthPriv or AuthNoPriv. This is the SNMPv3 authorization password. The default value is "admin123".
SNMPv3 Privacy Protocol	N/A	This parameter is applicable only if Security Level is set to AuthPriv. Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. • AES (default) • DES
SNMPv3 Priv Passphrase	8 to 32 characters.	This parameter is applicable only if Security Level is set to AuthPriv. This is the SNMPv3 privacy password. The default value is "admin123".
Management Client		
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.

Parameter	Length/Range	Description
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP (default) • REST

SNMPv3 Security Levels

SNMPv3 Security Level	SNMPv3 User	SNMPv3 Authentication Protocol	SNMPv3 Authentication Key	SNMPv3 Privacy Protocol	SNMPv3 Privacy Key
None	-	-	-	-	-
NoAuthNoPriv	✓	-	-	-	-
AuthNoPriv	✓	✓	✓	-	-
Authpriv	✓	✓	✓	✓	✓

Register a DELL Device

You can manually register DELL devices on the Ribbon Application Management Platform (RAMP).

Prerequisites

- The DELL device is up and running.
- RAMP IP address is configured in the DELL system parameters section.
- Super User [privileges](#) are available for Insight Administration under Core Resources.
- Devices and Resource Groups [privileges](#) under Device Management.

Start

Perform the following to register a DELL device:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **DELL**.
5. Configure the DELL registration parameters using the following table and click **Save**.

DELL Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the DELL device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register a DELL instance. • Node

Parameter	Length/Range	Description
Type	N/A	Select DELL as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters.	Provide a unique name for the node. Do not use special characters such as: <code>^[^<>.:;,+*?"'<> !@#\$\$%^&() `{}]*\$</code>.
Node IP		
Primary IP	N/A	Enter the default or primary IP address.
Secondary IP	N/A	Enter the default or secondary IP address.
SNMP Configuration		
Rediscover the devices after updating the SNMP configuration. Refer to Discover Nodes for details.		
SNMP Read Community	1 to 72 alphanumeric characters.	This is the community string for traps, resync, and reachability. If the community string is incorrect, DELL ignores the request and does not respond. If you change the value in RAMP, update this value on DELL. The default value is "public".

Parameter	Length/Range	Description
Port	N/A	The SNMP port number used for the device. The default port number is "161".
SNMPv3 Security Level	N/A	The parameter is applicable only for SNMPv3. Select the type of security model to apply to SNMP connections: • None (Default) – no security. • AuthPriv – authentication is required, and messages are encrypted. • AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private.
SNMPv3 User	5 to 32 alphanumeric characters.	Note This parameter is applicable only if the Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv Enter the username of the SNMPv3 user for authentication.
SNMPv3 Authentication Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. To enable private interactions over secure channels, select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol. • SHA (default) • MD5

Parameter	Length/Range	Description
SNMPv3 Auth Passphrase	8 to 32 characters.	This parameter is applicable only if Security Level is set to AuthPriv or AuthNoPriv. This is the SNMPv3 authorization password. The default value is "admin123".
SNMPv3 Privacy Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv. Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. • AES • DES (default)
SNMPv3 Priv Passphrase	8 to 32 characters.	This parameter is applicable only if the Security Level is set to AuthPriv. This is the SNMPv3 privacy password. The default value is "admin123".
Management Client		
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.

Parameter	Length/Range	Description
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP (Default) • REST

SNMPv3 Security Levels

SNMPv3 Security Level	SNMPv3 User	SNMPv3 Authentication Protocol	SNMPv3 Authentication Key	SNMPv3 Privacy Protocol	SNMPv3 Privacy Key
None	-	-	-	-	-
NoAuthNoPriv	✓	-	-	-	-
AuthNoPriv	✓	✓	✓	-	-
Authpriv	✓	✓	✓	✓	✓

Register a DSC Device

You can manually register DSC devices (DSC 8000 and DSC SWe) using the Ribbon Application Management Platform (RAMP).

Note

DSC SP2000/vSP2000 is not supported in RAMP 23.06 and later releases.

On the DSC web GUI:

- Enable EMS on the DSC GUI.
- Change the EMS type to EMS.

Prerequisites

- The DSC device is up and running.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

Perform the following procedure to register a DSC device:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **DSC**.
5. Configure the DSC registration parameters using the following table and click **Save**.

DSC Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the DSC device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register a single DSC instance. • Node

Parameter	Length/Range	Description
Type	N/A	Select DSC as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters.	Provide a unique name for the node. Do not use special characters such as: <code>^[^<>.:,+=*?\"<> !@#\$\$%^&() `{}]*\$</code>.
Node IP		
Primary IP	N/A	The shared/primary IP address of the DSC. Note The Primary IP address should be the slot 1 IP address of the DSC for DSC V23.01.00 or above.
Secondary IP	N/A	Enter the secondary IP address of the DSC. Note The Secondary IP address should be the slot 2 IP address of the DSC for DSC V23.01.00 or above.
Interfaces		
SFTP		

Parameter	Length/Range	Description
Username	1 to 49 alphanumeric characters.	Enter the SFTP login name to access the DSC through the RAMP. For the SFTP-based performance management collection to work, you must enable SSH and set the login name and password. The default value is "root".
Password	1 to 96 alphanumeric characters.	Enter the SFTP password. The default value is "y6U&i8o9".
SNMP Configuration		
Note Rediscover the devices after updating the SNMP configuration. Refer to Discover Nodes for details.		
Set Community	N/A	Enter the string that is sent along with each SNMP Set-Request. - If the community string is correct, the device responds with the requested information. - If the community string is incorrect, the device ignores the request and does not respond. The default value is "ins_ems".
Get Community	1 to 72 alphanumeric characters.	Enter the string that is sent along with each SNMP Get-Request. - If the community string is correct, the device responds with the requested information. - If the community string is incorrect, the device ignores the request and does not respond. If you change the value on the RAMP , update this value on the DSC device. Ribbon strongly recommends changing the default SNMP Community string for security reasons. The default value is "public".
SNMP Port	N/A	Enter the port number on the DSC to which RAMP should send the SNMP queries. The default port is "161".
Management Client		

Parameter	Length/Range	Description
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interfaces	N/A	Select the interface to use for reachability polling. • SNMP

Note

After an upgrade of the DSC from pre-23.01 to 23.01 or above, DSC works with a shared IP address until you discover the node because the DSC version on RAMP is still pre-23.01.

When RAMP discovers the node and identifies that the DSC version is 23.01 or above, then it expects the secondary IP address. If the secondary IP address is not present, the discovery fails. You must update the slot 1 IP address as the Primary IP address and slot 2 IP address as the secondary IP address and then discover the node.

Register a DSI Device

You can manually register DSI devices deployed on KVM or VMware on the Ribbon Application Management Platform (RAMP).

Prerequisites

Ensure that:

- The DSI device is up and running.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.
- MD5 must be enabled on RAMP.

Note

The RAMP supports only DSI version 12.x and above.

Start

Perform the following procedure to register a DSI device:

1. Log on to the [RAMP GUI](#).
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **DSI**.
5. Configure the DSI registration parameters using the following table and click **Save**.

DSI Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .

Parameter	Length/Range	Description
Resource Group	N/A	(Optional) Select a resource group to add the DSI device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register a single DSI instance. • Node
Type	N/A	Select DSI as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters. Do not use special characters like <code>^[^<>.:;,+*?"'<> !@#\$\$%^&(){}]*\$</code>	Provide a unique name for the node .
Node IP		
Primary IP	N/A	Enter the default or primary IP address of the DSI.
Secondary IP	N/A	Enter the secondary IP address. If the Primary IP is not the NFS IP of a GSX, then use this field to update the NFS IP that is needed for GSX to NFS communication.

Parameter	Length/Range	Description
Interfaces		
Agent		
Username	N/A	RAMP uses a DSI agent to communicate with DSI. If you have changed the default login on the device, enter the new agent login name. The default value is "admin".
Password	N/A	Enter the password for the DSI agent. Ribbon strongly recommends changing the default agent password for security reasons. If you change the default values on the RAMP, update these values on the DSI device. The default password is "admin".
SFTP		
Username	1 TO 49 alphanumeric characters.	Enter the SFTP login name to access the DSI through the RAMP SSH . The default value is "dsi".
Password	1 to 96 alphanumeric characters.	Enter the SFTP password to access the DSI. If the SFTP SSH password is not set, a passwordless login to the DSI is performed. If the password is not provided, ensure that passwordless SSH login is enabled from the RAMP to the DSI.
SNMP Configuration		
Note Rediscover the devices after updating the SNMP configuration. For more information, refer to Discover Nodes.		

Parameter	Length/Range	Description
Get Community	1 to 72 alphanumeric characters.	Enter the string that is sent along with each SNMP Get-Request. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device ignores the request and does not respond. If you change the value on the RAMP, update the changes on the DSI device. Ribbon strongly recommends changing the default SNMP Community string for security reasons. The default value is "yeix87493klup".
Trap Community	N/A	Enter the string that is included when the DSI sends SNMP Traps to the RAMP. Ribbon strongly recommends changing the default SNMP Trap Community string for security reasons. The default value is "hefj6483xhie".
SNMP Port	N/A	Enter the port number on the DSI to which RAMP should send the SNMP queries. The default port is "161".

Parameter	Length/Range	Description
SNMPv3 Security Level	N/A	Specifies the SNMPv3 security levels. The options are: • None (default) – no security. • AuthPriv– authentication is required, and messages are encrypted. • AuthNoPriv– connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv– users that connect with this level have no authentication, and the messages they send and receive are not private. If you edit an existing profile, the SNMP v3 fields are displayed based on the SNMP trap version selected and the value of the SNMP V3 Security Level. If the SNMPv3 Security Level is set to None then RAMP receives traps from the DSI as v2 traps. If the SNMPv3 Security Level is set to any other value other than None, then RAMP receives v3 traps from DSI. Note This parameter is applicable only for the SNMPv3.
SNMPv3 User	5 - 32 alphanumeric characters.	Enter the username of the SNMPv3 user for authentication. Note This parameter is applicable only if the Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv

Parameter	Length/Range	Description
SNMPv3 Authentication Protocol	N/A	To enable private interactions over secure channels, select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol. • MD5 (default) • SHA Note This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv.
SNMPv3 Auth Passphrase	8 to 32 alphanumeric characters.	This is the SNMPv3 authorization password. Note This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv.
SNMPv3 Privacy Protocol	N/A	Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. • AES (default) • DES Note This parameter is applicable only if the Security Level is set to AuthPriv.
SNMPv3 Priv Passphrase	8 to 32 alphanumeric characters.	The SNMPv3 privacy password. Note This parameter is applicable only if the Security Level is set to AuthPriv.

Parameter	Length/Range	Description
Management Client		
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP

Register a G5 Device

You can manually register G5 Line Access Gateway devices (G5) on the Ribbon Application Management Platform (RAMP).

Prerequisites

- The G5 device is up and running.
- The RAMP IP address is configured in the G5 system parameters section.
- [Super User](#) privileges for Insight Administration under Core Resources.
- Devices and Resource Groups [privileges](#) under Device Management.

Start

Perform the following procedure to register a G5 device:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **G5**.
5. Configure the G5 registration parameters using the following table and click **Save**.

G5 Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the G5 device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register a G5 instance. • Node

Parameter	Length/Range	Description
Type	N/A	Select G5 as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters.	Provide a unique name for the node. Do not use special characters such as: ^[^\<>.:;,+ = * ? \ " < > ! @ # \$ % ^ & () ` { }] * \$.
Node IP		
Primary IP	N/A	Enter the default or primary IP address.
Secondary IP	N/A	Enter the default or secondary IP address.
SNMP Configuration		
Rediscover the devices after updating the SNMP configuration. Refer to Discover Nodes for details.		
SNMP Read Community	1 to 72 alphanumeric characters.	This is the community string for traps, resync, and reachability. If the community string is incorrect, G5 ignores the request and does not respond. If you change the value in RAMP, update this value on G5 . The default value is "public".

Parameter	Length/Range	Description
SNMP Write Community	N/A	This is the community string for resync. If the community string is incorrect, G5 ignores the request and does not respond. If you change the value in RAMP, update this value on G5 .
Port	N/A	The SNMP port number used for the device. The default port number is "161".
SNMPv3 Security Level	N/A	The parameter is applicable only for SNMPv3. Select the type of security model to apply to SNMP connections: • None (Default) – no security. • AuthPriv– authentication is required, and messages are encrypted. • AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private.
SNMPv3 User	5 to 32 alphanumeric characters.	Note This parameter is applicable only if the Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv Enter the username of the SNMPv3 user for authentication.

Parameter	Length/Range	Description
SNMPv3 Authentication Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. To enable private interactions over secure channels, select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol. • SHA (default) • MD5
SNMPv3 Auth Passphrase	8 to 32 characters.	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. This is the SNMPv3 authorization password. The default value is "admin123".
SNMPv3 Privacy Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv. Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. • AES • DES (default)
SNMPv3 Priv Passphrase	8 to 32 characters.	This parameter is applicable only if the Security Level is set to AuthPriv. This is the SNMPv3 privacy password. The default value is "admin123".
Management Client		

Parameter	Length/Range	Description
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP (default) • REST

SNMPv3 Security Levels

SNMPv3 Security Level	SNMPv3 User	SNMPv3 Authentication Protocol	SNMPv3 Authentication Key	SNMPv3 Privacy Protocol	SNMPv3 Privacy Key
None	-	-	-	-	-
NoAuthNoPriv	✓	-	-	-	-
AuthNoPriv	✓	✓	✓	-	-
Authpriv	✓	✓	✓	✓	✓

Register a G6MM Device

You can manually register G6MM devices on the Ribbon Application Management Platform (RAMP).

Prerequisites

- The G6MM device is up and running.
- [Super User](#) privileges for Insight Administration under Core Resources.
- Devices and Resource Groups [privileges](#) under Device Management.

Start

Perform the following procedure to register a G6MM device:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **G6MM**.
5. Configure the G6MM registration parameters using the following table and click **Save**.

G6MM Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .

Parameter	Length/Range	Description
Resource Group	N/A	(Optional) Select a resource group to add the G6MM device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register a G6MM instance. • Node
Type	N/A	Select G6MM as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters. Do not use special characters like ^[\^<>.:;,+=*?"'<> !@#\$\$%^&() `{}]*\$	Provide a unique name for the node.
Node IP		
Primary IP	N/A	Enter the default or primary IP address.
Secondary IP	N/A	Enter the default or secondary IP address.
FQDN	N/A	Enter the Fully Qualified Domain Name (FQDN).

Parameter	Length/Range	Description
SNMP Configuration		
Rediscover the devices after updating the SNMP configuration. Refer to Discover Nodes for details.		
SNMP Read Community	1 to 72 alphanumeric characters.	This is the community string for traps, resync, and reachability. If the community string is incorrect, G6MM ignores the request and does not respond. If you change the value in RAMP, update this value on G6MM. The default value is "public".
Port	N/A	The SNMP port number used for the device. The default port number is "161".
SNMPv3 Security Level	N/A	Note SNMPv3 Security Levels are currently not supported for G6MM. The parameter is applicable only for SNMPv3. Select the type of security model to apply to SNMP connections: • None (Default) – no security. • AuthPriv– authentication is required, and messages are encrypted. • AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private.

Parameter	Length/Range	Description
SNMPv3 User	5 to 32 alphanumeric characters.	Note This parameter is applicable only if the Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv Enter the username of the SNMPv3 user for authentication.
SNMPv3 Authentication Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. To enable private interactions over secure channels, select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol. • SHA (default) • MD5
SNMPv3 Auth Passphrase	8 to 32 characters.	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. This is the SNMPv3 authorization password. The default value is "admin123".

Parameter	Length/Range	Description
SNMPv3 Privacy Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv. Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. • AES (default) • DES
SNMPv3 Priv Passphrase	8 to 32 characters.	This parameter is applicable only if the Security Level is set to AuthPriv. This is the SNMPv3 privacy password. The default value is "admin123".
Management Client		
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.

Parameter	Length/Range	Description
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP (default) • REST

SNMPv3 Security Levels

SNMPv3 Security Level	SNMPv3 User	SNMPv3 Authentication Protocol	SNMPv3 Authentication Key	SNMPv3 Privacy Protocol	SNMPv3 Privacy Key
None	-	-	-	-	-
NoAuthNoPriv	✓	-	-	-	-
AuthNoPriv	✓	✓	✓	-	-
Authpriv	✓	✓	✓	✓	✓

Register a GMS Device

You can manually register GMS devices on the Ribbon Application Management Platform (RAMP).

Prerequisites

- The GMS device is up and running.
- [Super User](#) privileges for Insight Administration under Core Resources.
- Devices and Resource Groups [privileges](#) under Device Management.

Start

Perform the following procedure to register a GMS device:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **GMS**.
5. Configure the GMS registration parameters using the following table and click **Save**.

GMS Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. The default value is "root". For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the GMS device to an existing resource group. • root • <any other existing tenants>
Device	N/A	Select Node to register a GMS instance. • Node

Parameter	Length/Range	Description
Type	N/A	Select GMS as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters. Do not use special characters like ^[^\<>.,;,+=*?"'<> !@#\$\$%^&() `{}]*\$	Provide a unique name for the node.
Node IP		
Primary IP	N/A	Enter the default or primary IP address.
Secondary IP	N/A	Enter the default or secondary IP address.
SNMP Configuration		
Rediscover the devices after updating the SNMP configuration. Refer to Discover Nodes for details.		
SNMP Read Community	1 to 72 alphanumeric characters.	This is the community string for traps, resync, and reachability. If the community string is incorrect, GMS ignores the request and does not respond. If you change the value in RAMP, update this value on GMS. The default value is "public".

Parameter	Length/Range	Description
Port	N/A	The SNMP port number used for the device. The default port number is "161".
SNMPv3 Security Level	N/A	The parameter is applicable only for SNMPv3. Select the type of security model to apply to SNMP connections: • None (Default) – no security. • AuthPriv– authentication is required, and messages are encrypted. • AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private.
SNMPv3 User	5 to 32 alphanumeric characters.	Note This parameter is applicable only if the Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv Enter the username of the SNMPv3 user for authentication.
SNMPv3 Authentication Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. To enable private interactions over secure channels, select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol. • SHA (default) • MD5

Parameter	Length/Range	Description
SNMPv3 Auth Passphrase	8 to 32 characters.	This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. This is the SNMPv3 authorization password. The default value is "admin123".
SNMPv3 Privacy Protocol	N/A	This parameter is applicable only if the Security Level is set to AuthPriv. Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. • AES (default) • DES
SNMPv3 Priv Passphrase	8 to 32 characters.	This parameter is applicable only if the Security Level is set to AuthPriv. This is the SNMPv3 privacy password. The default value is "admin123".
Management Client		

Parameter	Length/Range	Description
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes

Parameter	Length/Range	Description
Interface	N/A	Select the interface to use for reachability polling. • SNMP (default) • REST

SNMPv3 Security Levels

SNMPv3 Security Level	SNMPv3 User	SNMPv3 Authentication Protocol	SNMPv3 Authentication Key	SNMPv3 Privacy Protocol	SNMPv3 Privacy Key
None	-	-	-	-	-
NoAuthNoPriv	✓	-	-	-	-
AuthNoPriv	✓	✓	✓	-	-
Authpriv	✓	✓	✓	✓	✓

Register a GSX Device

You can manually register GSX devices deployed on KVM on the Ribbon Application Management Platform (RAMP).

Prerequisites

- The GSX device is up and running.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- Devices and Resource Groups [privileges](#) under **Device Management**.
- If GSX is running with weak ciphers and if you want to register a GSX device, follow the [Legacy Device Management](#) to enable ciphers

Start

Perform the following procedure to register a GSX device:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device as Node** and **Type as GSX**.
5. Configure the GSX registration parameters using the following table and **Save**.

GSX Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the GSX device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register a single GSX instance. • Node
Type	N/A	Select GSX as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters. Do not use special characters like <code>^[^<>.:,;+*=?"'<> !@#\$\$%^&() `{}]*\$</code>	Provide a unique name for the node.
Node IP		

Parameter	Length/Range	Description
Host 1 Default IP	N/A	Enter the default IP address of the GSX host 1.
Host 2 Default IP	N/A	Enter the default IP address of the GSX host 2.
Host 1 Secondary IP	N/A	Enter the secondary IP address of the GSX host 1.
Host 2 Secondary IP	N/A	Enter the secondary IP address of the GSX host 2.
Use Remote Agent	N/A	Select whether to use a remote agent. If this option is enabled during GSX registration, then Host 2 uses RAMP to access Call Trace and Call History records that are stored on the DSI. For this to work, the DSI should: • be registered with RAMP • have the Remote Agent installed. Otherwise, a warning message is displayed. Ensure that the RPC processes are running. If they are not, the Local Agent functionality will not work, and the NFS will not be mounted on RAMP while creating a call history report. • On (default) • Off
Interfaces		
SSH		
Enabled	N/A	Select this option to enable SSH secure communications. If this is enabled, RAMP captures SSH active channel and historical log information for the GSX nodes using SSH. • On (default) • Off
Telnet		
Username	1 to 49 alphanumeric characters.	Enter the username with administration level Telnet/CLI access to the GSX. The default value is "admin".

Parameter	Length/Range	Description
Password	1 to 96 alphanumeric characters.	Enter the password for the Telnet user. The default value is "gsx9000".
SNMP		
Note Rediscover the devices after updating the SNMP configuration. Refer to Discover Nodes for details.		
SNMP Read Community	1 to 72 alphanumeric characters.	Enter the string that is sent along with each SNMP Get-Request. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device ignores the request and does not respond. If you change the value in RAMP, update this value on the GSX device. The default value is "hefj6483xhie". Ribbon strongly recommends changing the default SNMP Community string for security reasons.
SNMP Write Community	N/A	Enter the string that is sent along with each SNMP Set-Request. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device ignores the request and does not respond. The default value is "yeix87493klup".
SNMP Trap Community	N/A	Enter the string that is included when the GSX sends SNMP traps to RAMP. Ribbon strongly recommends changing the default SNMP Trap Community string for security reasons. The default value is "hefj6483xhie".
SNMP Trap Type	N/A	Select the SNMP version. v2
Management Client		

Parameter	Length/Range	Description
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability Polling		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. - None 1 Minute (default) 2 Minutes 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. SNMP

Register an IDH Device

In this section:

- [Enable IDH on RAMP](#)

- [Register an IDH Device](#)

You can manually register Identity Hub (IDH) devices on the Ribbon Application Management Platform (RAMP). First, enable IDH on RAMP, then register IDH devices on RAMP.

For more information, refer to [Identity Hub Manager on RAMP](#).

Prerequisites

- Super User [privileges](#) for GUI and Configuration Management under Core Resources.
- Devices and Resource Groups [privileges](#) under Device Management.

Enable IDH on RAMP

Perform this procedure to enable IDH on the RAMP:

Start

1. Log on to the RAMP GUI.
2. Navigate to **System > Settings > RAMP Profile Settings**.
3. In the **Global Node Type Registration**, enable **IDH**.
4. Click **Save Settings**.

Register an IDH Device

Perform this procedure to register an IDH device on the RAMP:

Start

1. Navigate to **DEVICE MANAGEMENT > Devices**.
2. Click **Add Devices**. The **Add Device** window displays.
3. Select the **Device** as **Node** and **Type** as **IDH**.
4. Configure the IDH registration parameters using the following table and click **Save**.

IDH Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the STI device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register an STI instance. • Node

Parameter	Length/Range	Description
Type	N/A	Select IDH as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Service Information		
Service Name	1 to 64 characters. Do not use special characters like <code>^[^<>:;,+=*?"'<> !@#\$\$%^&() `{}]*\$</code>	Provide a unique name for the service.
Service URL	N/A	The FQDN for accessing the Identity Hub service provided by Ribbon as part of the onboarding process. For example, <code>https://<idhub-service-fqdn.com></code> .
Service URL Parameters	N/A	Your unique tenant identifier provided by Ribbon as part of the onboarding process. The format to enter the tenant identifier is, <code>tenant=<your tenant ID></code> . For example, <code>tenant=abc123XyZ</code>

Parameter	Length/Range	Description
Management Access Token	N/A	The management access key for the Identity Hub service provided by Ribbon provided as part of the onboarding process. Or, if you already have a new management access key (also known as the management API key) to submit REST API requests, enter the current management API key in this field. The Identity Hub service stores a single management API key/access token value for authorizing management actions. Use the current value to submit management requests for either the REST API or the Identity Hub Manager. Note If the management access token is deleted from Service Information for any reason and you do not have a copy of the value to restore it, contact Ribbon Support for assistance in resetting the access token.
Supplementary Service Parameters	N/A	Additional parameters to add to the IDH launch URL. This option is not currently used and left blank.
Management Client		
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.

Parameter	Length/Range	Description
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
General		
Reachability Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • REST

Register an L2MGR Device

You can manually register L2MGR devices on the Ribbon Application Management Platform (RAMP).

Prerequisites

- The L2MGR device is up and running.
- RAMP IP address is configured in the L2MGR system parameters section.
- [Super User](#) privileges for Insight Administration under Core Resources.
- Devices and Resource Groups [privileges](#) under Device Management.

Start

Perform the following procedure to register an L2MGR device:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **L2MGR**.
5. Configure the L2MGR registration parameters using the following table and click **Save**.

L2MGR Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the L2MGR device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register an L2MGR instance. • Node
Type	N/A	Select L2MGR as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters. Do not use special characters like ^[\^<>.:;,+=*?"'<> !@#\$\$%^&() `{}]*\$	Provide a unique name for the node.

Parameter	Length/Range	Description
Node IP		
Primary IP	N/A	Enter the default or primary IP address.
Secondary IP	N/A	Enter the default or secondary IP address.
SNMP Configuration		
Rediscover the devices after updating the SNMP configuration. Refer to Discover Nodes for details.		
SNMP Read Community	1 to 72 alphanumeric characters.	This is the community string for traps, resync, and reachability. If the community string is incorrect, L2MGR ignores the request and does not respond. If you change the value in RAMP, update this value on L2MGR. The default value is "public".
Port	N/A	The SNMP port number used for the device. The default port number is "161".
SNMPv3 Security Level	N/A	The parameter is applicable only for SNMPv3. Select the type of security model to apply to SNMP connections: • None (Default) – no security. • AuthPriv – authentication is required, and messages are encrypted. • AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private. The default value is "None".

Parameter	Length/Range	Description
SNMPv3 User	5 to 32 alphanumeric characters.	Enter the username of the SNMPv3 user for authentication. Note This parameter is applicable only if the Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv
SNMPv3 Authentication Protocol	N/A	Note This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. To enable private interactions over secure channels, select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol. • SHA (default) • MD5
SNMPv3 Auth Passphrase	8 to 32 characters.	Note This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv. This is the SNMPv3 authorization password. The default value is "admin123".

Parameter	Length/Range	Description
SNMPv3 Privacy Protocol	N/A	Note This parameter is applicable only if the Security Level is set to AuthPriv. Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. • AES (default) • DES
SNMPv3 Priv Passphrase	8 to 32 characters.	Note This parameter is applicable only if the Security Level is set to AuthPriv. This is the SNMPv3 privacy password. The default value is "admin123".
Management Client		
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.

Parameter	Length/Range	Description
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP (default) • REST

SNMPv3 Security Levels

SNMPv3 Security Level	SNMPv3 User	SNMPv3 Authentication Protocol	SNMPv3 Authentication Key	SNMPv3 Privacy Protocol	SNMPv3 Privacy Key
None	-	-	-	-	-
NoAuthNoPriv	✓	-	-	-	-
AuthNoPriv	✓	✓	✓	-	-
Authpriv	✓	✓	✓	✓	✓

Register a PSX Device

In this section:

- [Manually Register a PSX Device](#)
- [GR Support for Non-Cloud Environment \(KVM and VMware\) PSX](#)

You can manually register PSX devices deployed on KVM or VMware running PSX 14.x and earlier on the Ribbon Application Management Platform (RAMP).

You can also modify a manually-registered Primary PSX to become the Replica, and vice-versa.

Note

The PSX 15.x and later releases do not support manually registering devices across platforms (including KVM and VMware) because the PSX must be part of a cluster and only dynamic registration is supported.

Prerequisites

- The PSX device is up and running.
- Read and write [privileges](#) under **PSX Management**.
- Devices and Resource Groups [privileges](#) under **Device Management**.

Manually Register a PSX Device

Perform the following procedure to manually register a PSX device on the RAMP:

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **PSX**.
5. Configure the PSX registration parameters using the following table and click **Save**.

PSX Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .

Parameter	Length/Range	Description
Resource Group	N/A	(Optional) Select a resource group to add the PSX device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register a single PSX instance. • Node
Type	N/A	Select PSX as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters.	Provide a unique name for the node. (Do not use special characters like ^[<>:,;,+ = * ? \ " < > ! @ # \$ % ^ & () ` { }] * \$)
Primary / Replica	N/A	Set whether the PSX is a primary or replica. A replica PSX device must reference a primary PSX (below). • Primary • Replica
Primary PSX Name	N/A	If the PSX is a replica, then select the Primary PSX Name . Name of the PSX to act as primary for this PSX. NOTE: This parameter is applicable only for PSX replica nodes.

Parameter	Length/Range	Description
Redundancy Type	N/A	This is the deployment model. If you are deploying the PSX as a standalone instance, select Standalone. If it is part of a high availability configuration, select HA. • Standalone (default) • HA
Database SID	N/A	The database SID (system identifier) on the PSX.
SSREQ	N/A	The port on RAMP to use for launching the SoftSwitch Request (SSREQ) tool. The default value is "3091".
Test DB Only	N/A	Set whether to use the PSX with a test database.
Test DB Mgmt Port	N/A	NOTE: This parameter is applicable only if the Test DB Only checkbox is selected. The port number on RAMP to access the test database. The default value is "4331".
Node IP		
Primary IP	N/A	The default or primary IP address of the standalone PSX. This parameter is applicable only if the Redundancy Type is set as Standalone.
Secondary IP	N/A	The secondary IP address of the standalone PSX. This parameter is applicable only if the Redundancy Type is set as Standalone.
Logical IP	N/A	Enter the logical IP address of the HA PSX. This parameter is applicable only if the Redundancy Type is set as HA.
Host 1 Primary IP	N/A	Enter the Host1 Primary IP address of the HA PSX. This parameter is applicable only if the Redundancy Type is set as HA.

Parameter	Length/Range	Description
Host 2 Primary IP	N/A	Enter the Host 2 Primary IP address of the PSX. This parameter is applicable only if the Redundancy Type is set as HA .
Interfaces		
Note For HA, both active and standby nodes should have the same credentials for each connection interface.		
Agent		
Username	1 to 49 alphanumeric characters.	RAMP uses a PSX Agent to communicate with a PSX. If you have changed the default login on the PSX device, enter the Agent Login name. The default value is "admin".
Password	1 to 96 alphanumeric characters.	The password for PSX Agent. If you have changed the default values on the PSX device, enter the Agent Password. The default value is "admin".
Management		
Username	1 to 49 alphanumeric characters.	Enter the PSX Policy Information Provisioning Engine (PIPE) username. NOTE: The parameter is applicable only for a primary PSX node.
Password	1 to 49 alphanumeric characters.	Enter the password for PSX PIPE.
Port		The management port on RAMP to use for managing the PSX device. The default value is "4330".
SSH		

Parameter	Length/Range	Description
SSH Enabled	N/A	Select this option to enable Secure Shell Protocol (SSH) secure communications between RAMP and the PSX. • On (default) • Off NOTE: Enable SSH and set the login name and password to enable SFTP-based performance management collection to work. Note • If the SSH Enabled checkbox is not selected, ensure that the TCP/EGRESS 4330 port is enabled on RAMP for successful PSX node discovery. • If the SSH Enabled checkbox is not selected then the following message displays "The communication to PSX is not secure, enable SSH to secure communication".
Username	1 to 49 alphanumeric characters.	Specifies The SSH login name for accessing the PSX through RAMP. The default value is "ssuser". NOTE: This parameter is applicable only if SSH is enabled. NOTE: Enable SSH and set the login name and password for the SFTP-based performance management collection to work.
Password	1 to 49 alphanumeric characters.	Specifies the SSH password to access the PSX. NOTE: This parameter is applicable only if SSH is enabled.
Strict Mode	N/A	The Strict Mode option is visible only if SSH is enabled. Select the strict mode to enhance security. If strict mode is enabled, the fingerprints of the device are collected and stored in the database. The SSH connection is established only after validating the fingerprint of the device against the stored entry in RAMP.

Parameter	Length/Range	Description
Database		
Username	1 to 49 alphanumeric characters.	The username to access the PSX database. The default value is "insightuser".
Password	1 to 49 alphanumeric characters.	The password to access the PSX database. The default value is "insightuser".
Port	N/A	The port number to access the PSX database. The default value is "1521".
SNMP Configuration		
Rediscover the devices after updating the SNMP configuration. Refer to Discover Nodes for details.		
SNMP Read Community	1 to 72 alphanumeric characters.	Enter the SNMP Read Community String. Ribbon strongly recommends changing the default SNMP Community strings for security reasons. The default value is "hefj6483xhie".
Port Number	N/A	Enter the port number on the PSX to which RAMP should send SNMP queries. The default value is "161".

Parameter	Length/Range	Description
SNMPv3 Security Level	N/A	The parameter is applicable only for SNMPv3. Select the type of security model to apply to SNMP connections: • None (Default) – no security. • AuthPriv– authentication is required, and messages are encrypted. • AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private.
SNMPv3 User	5 to 32 alphanumeric characters.	Enter the username of the SNMPv3 user for authentication. Note This parameter is applicable only if the Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv
SNMPv3 Authentication Protocol	N/A	To enable private interactions over secure channels, select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol. • MD5 (default) • SHA Note This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv.

Parameter	Length/Range	Description
SNMPv3 Auth Passphrase	8 to 32 characters.	Specifies the SNMPv3 authorization password. Note This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv.
SNMPv3 Privacy Protocol	N/A	Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) as the authentication protocol. • AES (default) • DES Note This parameter is applicable only if the Security Level is set to AuthPriv.
SNMPv3 Priv Passphrase	8 to 32 characters.	Specifies the SNMPv3 privacy password. Note This parameter is applicable only if the Security Level is set to AuthPriv.
Management Client		

Parameter	Length/Range	Description
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP (default) • REST

GR Support for Non-Cloud Environment (KVM and VMware) PSX

Perform this procedure to promote a GR Replica PSX to the Primary PSX.

Start

1. Configure a PSX Cluster for Geographically Redundant (GR) support on the PSX. Refer to [GR Support for Non-Cloud Environment - KVM and VMware](#).
2. Promote the GR Replica PSX to be the Primary PSX. Refer to [GR Support for Non-Cloud Environment - KVM and VMware](#).
3. To modify the Replica PSX to be the Primary PSX:
 - a. Edit the manually registered PSX device:
 - i. Navigate to **DEVICE MANAGEMENT > Devices**. Refer to, [Edit RAMP Device Registration](#).
 - ii. In the Nodes list row for the PSX you want to edit, select the pencil icon under **Action** to open the edit page.

Some parameters can no longer be changed. Options that are no longer editable appear as read-only text on the Edit window.

- iii. The **EditReplicaPSX** window displays.
 - iv. In the menu for **Primary/Replica**, select **Primary**.
 - v. If you want to edit any other parameters, refer to the parameters table on the [Edit RAMP Device Registration](#) page.
 - vi. Click **Save** to remove the association of the Replica from the Primary.
 - vii. Discover the new Primary PSX:
 1. In the Nodes list row for the new Primary PSX, click the ellipses (...) menu under **Action** and select **Discover**.
4. If there are any other Replica PSX nodes, edit and associate them to the new Primary PSX.
5. Convert the old Primary PSX to be the Replica PSX. Refer to [GR Support for Non-Cloud Environment - KVM and VMware](#).
6. To modify the Primary PSX to be Replica PSX:
 - a. Edit the Replica PSX device:
 - i. Navigate to **DEVICE MANAGEMENT > Devices**. Refer to, [Edit RAMP Device Registration](#).
 - ii. In the Nodes list row for the PSX you want to edit, select the pencil icon under **Action** to open the edit page.

Some parameters can no longer be changed. Options that are no longer editable appear as read-only text on the Edit window.

- iii. The **EditPrimaryPSX** window displays.
 - iv. In the menu for **Primary/Replica**, select **Replica**. Select the Primary PSX.
 - v. If you want to edit any other parameters, refer to the parameters table on the [Edit RAMP Device Registration](#) page.
 - vi. Click **Save**. This associates the Replica PSX to the Primary PSX.
 - vii. Discover the new Replica PSX:
 1. In the Nodes list row for the new Primary PSX, click the ellipses (...) menu under **Action** and select **Discover**.
7. If needed, disassociate the node locked CPS licenses from the new Primary (old Replica) PSX and associate it to the new the Replica (old Primary) PSX,

Register an SBC Core Device

You can manually register SBC devices deployed on KVM or VMware on the Ribbon Application Management Platform (RAMP).

Prerequisites

- The SBC Core device is up and running.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

Perform the following procedure to register an SBC device on the RAMP:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **SBC Core**.
5. Configure the SBC registration parameters using the following table and click **Save**.

Click to view the SBC Core Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the SBC Core device to an existing resource group.
Device	N/A	Select Node to register a single SBC Core instance. • Node

Parameter	Length/Range	Description
Type	N/A	Select SBC Core as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters. Do not use special characters like <code>^[^<>.:,;+*=*\\"<> !@#%\$%^&() `{}]*\$</code>	Provide a unique name for the node.
Cluster	N/A	(Optional) Use this option to select an integrated SBC cluster on RAMP to which you want to add this node. You must add the node to a cluster when you register it. If added to a cluster, the node's traps and performance statistics are displayed along with other nodes in the cluster. Once a non-cloud SBC node is added to a cluster, you cannot delete the cluster until the device is deleted. To delete it, the registered device must be unregistered. Note If you include this device in a cluster, the SNMP Configuration and Reachability fields are no longer configurable. The node inherits those configurations from the cluster.

Parameter	Length/Range	Description
Redundancy Type	N/A	This is the deployment model. If you are deploying the SBC Core as a standalone instance, select Standalone . If it is part of a high availability configuration, select HA . The default value is "Standalone".
Node IP		
Primary IP	N/A	This parameter is applicable only if the Redundancy Type is set as Standalone . Enter the default or primary IP address of the SBC.
Secondary IP	N/A	This parameter is applicable only if the Redundancy Type is set as Standalone . Enter the default or secondary IP address of the SBC.
Host 1 Primary IP	N/A	This parameter is applicable only if the Redundancy Type is set as HA . Enter the Host1 Primary IP address of the SBC.
Host 1 Secondary IP	N/A	This parameter is applicable only if the Redundancy Type is set as HA . Enter the Host 1 Secondary IP address of the SBC.
Host 2 Primary IP	N/A	This parameter is applicable only if the Redundancy Type is set as HA . Enter the Host 2 Primary IP address of the SBC.
Host 2 Secondary IP	N/A	This parameter is applicable only if the Redundancy Type is set as HA . Enter the Host 2 Secondary IP address of the SBC.

Parameter	Length/Range	Description
Alternate IP	N/A	The non-cloud SBC Core's logical interfaces are discovered automatically and displayed as Alternate IP on the Node Overview page. This is to support traps from the logical IP of SBC Core.
Interfaces		
For HA, both active and standby nodes should have the same credentials for each connection interface.		
Netconf		
Username	1 to 49 alphanumeric characters.	Enter the NETCONF user name. The default user name is "admin".
Password	1 to 96 alphanumeric characters.	Enter the NETCONF password. The default password is "Sonus@123".
Port	N/A	Enter the port number to use for NETCONF access on the SBC device. The default value is "2022".
SSH		
Username	1 to 49 alphanumeric characters.	Enter the SSH login name for the SBC device. Set the SSH credentials to enable Call Trace and Call History for the SBC device in RAMP . The default value is "admin".
Password	1 to 96 alphanumeric characters.	Enter the SSH password for the SBC device. Note Ensure the user account has SSH and SFTP permissions on the SBC. Otherwise, functions such as Call Trace and Call History do not work.

Parameter	Length/Range	Description
Port	N/A	Enter the port number to use for SSH access on the SBC device. The default value is 2024.
Strict Mode	N/A	Select Strict Mode to enhance security. If you enable strict mode, the device's fingerprint is collected and stored in the database. An SSH connection is established only after validating the device's fingerprint against the stored entry in RAMP. By default, this mode is disabled.
LI		
Username	1 to 49 alphanumeric characters.	Enter a username for a lawful intercept (LI) user on the SBC device. The default value is "calea".
Password	1 to 96 alphanumeric characters.	Enter a password for the LI user on the device.
REST		
Port	N/A	Enter the port number to use for REST requests to the device. The default value is "444".
SNMP Configuration		
Note Rediscover the devices after updating the SNMP configuration. For more information, refer to Discover Nodes.		
SNMP Read Community	1 to 72 alphanumeric characters.	Enter the SNMP Read Community String. Ribbon strongly recommends changing the default SNMP Community strings for security reasons. The default value is "hefj6483xhie".
SNMP Port	N/A	Enter the port number on the SBC to which the RAMP should send SNMP queries. The default value is "161".

Parameter	Length/Range	Description
SNMPv3 Security Level	N/A	The parameter is applicable only for SNMPv3. Select the type of security model to apply to SNMP connections: • None (Default) – no security. • AuthPriv– authentication is required, and messages are encrypted. • AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private.
SNMPv3 User	5 to 32 alphanumeric characters.	Enter the username of the SNMPv3 user for authentication. Note This parameter is applicable only if the Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv

Parameter	Length/Range	Description
SNMPv3 Authentication Protocol	N/A	To enable private interactions over secure channels, select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol. • MD5 (default) • SHA Note If you register a JTIC enabled SBC on a JTIC enabled RAMP, then MD5 is not supported. Note This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv.
SNMPv3 Auth Passphrase	8 to 32 characters.	This is the SNMPv3 authorization password. Note This parameter is applicable only if the Security Level is set to AuthPriv or AuthNoPriv.

Parameter	Length/Range	Description
SNMPv3 Privacy Protocol	N/A	Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. • AES (default) • DES Note If you register a JTIC enabled SBC on a JTIC enabled RAMP, then DES is not supported. Note This parameter is applicable only if the Security Level is set to AuthPriv.
SNMPv3 Priv Passphrase	8 to 32 characters.	This is the SNMPv3 privacy password. Note This parameter is applicable only if the Security Level is set to AuthPriv.
Management Client		
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.

Parameter	Length/Range	Description
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP • REST (default)

SNMPv3 Security Levels

SNMPv3 Security Level	SNMPv3 User	SNMPv3 Authentication Protocol	SNMPv3 Authentication Key	SNMPv3 Privacy Protocol	SNMPv3 Privacy Key
None	-	-	-	-	-
NoAuthNoPriv	✓	-	-	-	-
AuthNoPriv	✓	✓	✓	-	-

SNMPv3 Security Level	SNMPv3 User	SNMPv3 Authentication Protocol	SNMPv3 Authentication Key	SNMPv3 Privacy Protocol	SNMPv3 Privacy Key
Authpriv	✓	✓	✓	✓	✓

Register an SGX Device

You can manually register SGX devices deployed on KVM on the Ribbon Application Management Platform (RAMP).

Prerequisites

- The SGX device is up and running.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- Devices and Resource Groups [privileges](#) under **Device Management**.

Start

Perform the following procedure to register an SGX device on the RAMP:

1. Log on to the [RAMP GUI](#).
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **SGX**.
5. Configure the SGX registration parameters using the following table and click **Save**.

SGX Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the SGX device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register a single SGX instance. • Node

Parameter	Length/Range	Description
Type	N/A	Select SGX as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters. Do not use special characters like <code>^[^<>.:,;+*=*\\"<> !@#\$\$%^&(){}]*\$</code>	Provide a unique name for the node.
Host 1		
Default IP Address	N/A	Enter the default IP address of the SGX host 1.
Second IP Address	N/A	Enter the second IP address of the SGX host 1.
Host 2		
Default IP Address	N/A	Enter the default IP address of the SGX host 2.
Second IP Address	N/A	Enter the second IP address of the SGX host 2.
Interfaces		
NETCONF		

Parameter	Length/Range	Description
Username	1 to 49 alphanumeric characters.	RAMP uses a NETCONF Interface to communicate with the SGX. If you have changed the default login on the device, enter the new username. The default value is "admin".
Password	N/A	The password for the NETCONF interface. If you have changed the default values on the device, enter the new password. The default password is "admin". Ribbon strongly recommends changing the default NETCONF password for security reasons. If you change the value in RAMP, update these values in the SGX device.
Port	N/A	Enter the port number to use for NETCONF access to the device. The default value is "2022".
CLI		
Username	1 to 49 alphanumeric characters.	Enter the command line interface (CLI) login name to access the SGX. The default value is "admin".
Password	N/A	Enter the password to access the SGX CLI. The default value is "admin".
SNMP Configuration		
Rediscover the devices after updating the SNMP configuration. Refer to Discover Nodes for details.		
SNMP Get Community	1 to 72 alphanumeric characters.	Enter the string that is sent along with each SNMP Get-Request. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device ignores the request and does not respond. If you change the value on RAMP, update this value on the SGX device. The default value is "hefj6483xhie". Ribbon strongly recommends changing the default SNMP Community string for security reasons.

Parameter	Length/Range	Description
SNMP Port	N/A	Enter the port number on the SGX to which the RAMP should send SNMP queries. The default value is "161".
Management Client		
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address . By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address . By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP

Register an SLB Device

You can manually register SLB devices deployed on KVM or VMware on the Ribbon Application Management Platform (RAMP).

Prerequisites

- The SLB device is up and running.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- Devices and Resource Groups [privileges](#) under **Device Management**.

Start

Perform the following procedure to register an SLB device:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Node** and **Type** as **SLB**.
5. Configure the SLB registration parameters using the following table and click **Save**.

SLB Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the SLB device to an existing resource group. • root • <any other existing resource group>
Device	N/A	Select Node to register a single SLB instance. • Node

Parameter	Length/Range	Description
Type	N/A	Select SLB as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Node Information		
Name	1 to 64 characters. Do not use special characters like <code>^[^<>,:;,+=*?"'<> !@#%\$%^&(){}]*\$</code>	Provide a unique name for the node.
Cluster	N/A	(Optional) Use this option to select an SLB cluster on RAMP to which you want to add this node. You must add the node to a cluster when you register it. If added to a cluster, the node's traps and performance statistics are displayed along with other nodes in the cluster. Once a non-cloud SLB node is added to a cluster, you cannot delete the cluster until the device is deleted. To delete it, the registered device must be unregistered. If you include this device as part of a cluster, then the SNMP Configuration and Reachability fields are no longer configurable. The node inherits those configurations from the cluster.

Parameter	Length/Range	Description
Redundancy Type	N/A	This is the deployment model. If you are deploying the SLB as a standalone instance, select Standalone. If it is part of a high availability configuration, select HA. • Standalone (default) • HA
Node IP		
Primary IP	N/A	Enter the default or primary IP address of the SLB. This parameter is applicable only if the Redundancy Type is set as Standalone.
Secondary IP	N/A	Enter the default or secondary IP address of the SLB. This parameter is applicable only if the Redundancy Type is set as Standalone.
Host 1 Primary IP	N/A	Enter the Host 1 Primary IP address of the SLB. This parameter is applicable only if the Redundancy Type is set as HA.
Host 1 Secondary IP	N/A	Enter the Host 1 secondary IP address of the SLB. This parameter is applicable only if the Redundancy Type is set as HA.
Host 2 Primary IP	N/A	Enter the Host 2 primary IP address of the SLB. This parameter is applicable only if the Redundancy Type is set as HA.
Host 2 Secondary IP	N/A	Enter the Host 2 secondary IP address of the SLB. This parameter is applicable only if the Redundancy Type is set as HA.

Parameter	Length/Range	Description
Interfaces		
For HA, both active and standby nodes should have the same credentials for each connection interface.		
Netconf		
Username	1 to 49 alphanumeric characters.	Enter the NETCONF user name. The default user name is "admin".
Password	1 to 96 alphanumeric characters.	Enter the NETCONF password. The default password is "Sonus@123".
Port	N/A	Enter the port number to use for NETCONF access on the SLB device. The default value is "2022".
SSH		
Username	1 to 49 alphanumeric characters.	Enter the SSH login name for the SLB device.
Password	1 to 96 alphanumeric characters.	Enter the SSH password for the SLB device.
Port	N/A	Enter the port number to use for SSH access on the SLB device. The default value is "2024".
Strict Mode	N/A	Select Strict Mode to enhance security. If you enable strict mode, the device's fingerprint is collected and stored in the database. An SSH connection is established only after validating the device's fingerprint against the stored entry RAMP. By default this mode is disabled.
LI		
Username	N/A	Enter a username for a lawful intercept (LI) user on the SLB device. The default value is "calea".

Parameter	Length/Range	Description
Password	N/A	Enter a password for the LI user on the device.
REST		
Port	N/A	Enter the port number to use for REST requests to the SLB device. The default value is "444".
SNMP Configuration		
Note Rediscover the devices after updating the SNMP configuration. For more information, refer to Discover Nodes.		
SNMP Read Community	1 to 72 alphanumeric characters.	Enter the SNMP Read Community String. Ribbon strongly recommends changing the default SNMP Community strings for security reasons. The default value is "hefj6483xhie".
SNMP Port	N/A	Enter the port number on the SLB to which RAMP should send SNMP queries. The default value is "161".

Parameter	Length/Range	Description
SNMP V3 Security Level	N/A	The parameter is applicable only for SNMPv3. Select the type of security model to apply to SNMP connections: • None (Default) – no security. • AuthPriv– authentication is required, and messages are encrypted. • AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private. • None (default) • AuthPriv • AuthNoPriv • NoAuthNoPriv
SNMPv3 User	5 to 32 alphanumeric characters.	Note This parameter is applicable only if Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv Enter the username of the SNMPv3 user for authentication.
SNMPv3 Authentication Protocol	N/A	This parameter is applicable only if Security Level is set to AuthPriv or AuthNoPriv. Select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol to enable private interactions over secure channels. • MD5 (default) • SHA

Parameter	Length/Range	Description
SNMPv3 Auth Passphrase	8 to 32 characters.	This parameter is applicable only if Security Level is set to AuthPriv or AuthNoPriv. This is the SNMPv3 authorization password.
SNMPv3 Privacy Protocol	N/A	This parameter is applicable only if Security Level is set to AuthPriv. Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. • AES (default) • DES
SNMPv3 Priv Passphrase	8 to 32 characters.	This parameter is applicable only if Security Level is set to AuthPriv. This is the SNMPv3 privacy password.
Management Client		
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.

Parameter	Length/Range	Description
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
Reachability		
Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • SNMP (default) • REST

SNMPv3 Security Levels

SNMPv3 Security Level	SNMPv3 User	SNMPv3 Authentication Protocol	SNMPv3 Authentication Key	SNMPv3 Privacy Protocol	SNMPv3 Privacy Key
None	-	-	-	-	-
NoAuthNoPriv	✓	-	-	-	-
AuthNoPriv	✓	✓	✓	-	-
Authpriv	✓	✓	✓	✓	✓

Register an STI Device

In this section:

- [Enable STI on RAMP](#)
- [Register an STI Device](#)

You can manually register Secure Telephony Identity (STI) devices on the Ribbon Application Management Platform (RAMP). First, enable STI on the RAMP, and then register the STI devices.

For more information, refer to [Accessing STI Manager from RAMP](#).

Prerequisites

- Super User [privileges](#) for GUI and Configuration Management under Core Resources.
- Devices and Resource Groups [privileges](#) under Device Management.

Enable STI on RAMP

Perform the following procedure to enable STI on RAMP:

Start

1. Log on to the RAMP GUI.
2. Navigate to **System > Settings > RAMP Profile Settings**.
3. In the **Global Node Type Registration**, enable **STI**.
4. Click **Save Settings**.

Register an STI Device

Perform the following procedure to register an STI device on the RAMP:

Start

1. Navigate to **DEVICE MANAGEMENT > Devices**.
2. Click **Add Devices**. The **Add Device** window displays.
3. Select the **Device** as **Node** and **Type** as **STI**.
4. Use the following table to configure the STI registration parameters and click **Save**.

STI Registration Parameters

Parameter	Length/Range	Description
Device Details		
Tenant	N/A	Used to implement multi-tenancy. • root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .
Resource Group	N/A	(Optional) Select a resource group to add the STI device to an existing resource group. • root • <any other existing resource group>

Parameter	Length/Range	Description
Device	N/A	Select Node to register an STI instance. • Node
Type	N/A	Select STI as the device type. • C20 • C3 • G9EMS • DELL • DSC • DSI • G5 • G6MM • GMS • GSX • IDH • L2MGR • PSX • RAMP • SBC Core • SGX • SLB • STI
Service Information		
Service Name	1 to 64 characters. Do not use special characters like <code>^[^<>.:;,+=*?\"<> !@#\$\$%^&() `{}]*\$</code>	Provide a unique name for the node.
Service URL	N/A	The management IP address or FQDN for the STI service. If you enter an IP address, use the format: <code>https://<management IP>:8080</code> . For example, <code>https://10.11.12.13:8080</code> .

Parameter	Length/Range	Description
Management Access Token	N/A	The administrative API key (access token) for authorizing requests to configure STI. If you already have an administrative API key generated to submit REST API requests, enter the current administrative API key in this field. Alternatively, click Generate Access Token to generate an initial administrative API key (access token) for the STI. The generated key is displayed in a pop-up window. Copy this key into the Management Access Token field and store a copy of the value in a secure location. On entering the key into the Management Access Token field, the key appears as a series of dots. NOTE: • The option to Generate Access Token is available when you register the device initially. Later, if you want to rotate or update the token, populate the Management Access Token field with the current access token when you make the request. • If the access token is deleted from Service Information for some reason and you do not have a copy of the value to restore it, contact Ribbon Support for assistance in resetting the access token. • The STI service stores a single administrative API key/access token value for authorizing configuration of the STI service for either the REST API or the STI Manager to submit the requests. If you generate an access token as part of registration with RAMP, you must use the same value as the administrative API key to authorize any subsequent requests made using the STI management REST API.
Supplementary Service Parameters	N/A	Additional parameters to add to the STI launch URL. This option is not currently used and left blank.
Management Client		

Parameter	Length/Range	Description
Address	IPv4 or IPv6 address format.	Lists the RAMP's primary and secondary IP addresses (if it has a secondary interface). You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
GR Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if it has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client GR Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address.
General		
Reachability Polling Interval	N/A	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes
Interface	N/A	Select the interface to use for reachability polling. • REST

Automatically Register Devices on RAMP

In this section:

- [Register C20 Devices](#)
- [Register an Edge 8000 Device](#)
- [Register an SBC Edge Device](#)
- [Register an EdgeMarc Device](#)

Ribbon Application Management Platform (RAMP) supports automatic registration of devices. Refer to the pages in this section for procedures to automatically register devices on RAMP.

For SBC Edge, you must deploy the EdgeView (EV) service on RAMP and ensure that the RAMP system is registered.

For C20 devices, you must register it to RAMP over the REST interface.

Register C20 Devices

C20 Call Session Controller (C20) devices can register automatically on Ribbon Application Management Platform (RAMP). Configure the C20 using the CLI menu on the device and register it to RAMP over the REST interface. For more information, refer to [C20 Auto Registration](#).

If you prefer to manually register C20 devices on RAMP, refer to [Register a C20 Device](#).

Register an Edge 8000 Device

The Ribbon Application Management Platform (RAMP) supports dynamic registration of Edge 8000 devices.

Edge 8000 Registration

On Edge 8000 Family

The Edge 8000 devices automatically register with RAMP after you complete the prerequisite configuration. The prerequisite configuration is to provide the RAMP IP address to each Edge 8000 device.

To register an Edge 8000 device with RAMP:

1. Log on to the GUI.
2. Set the RAMP server address.
3. Click the **Settings** tab.
4. Navigate to **System > Node-Level Settings**, select **Yes** from the pull-down menu in the **Connect to RAMP** field.
5. Enter the **Management Address** to set the RAMP server address to the IPv4 address or fully qualified domain name (FQDN) of the RAMP server.

On RAMP

To successfully manage Edge 8000 devices on RAMP before they attempt to register, you must deploy the EdgeView (EV) service on RAMP. To deploy the EdgeView service, refer to [Deploy Optional Services on RAMP](#).

To launch an Edge 8000 GUI from RAMP, refer to [Launch Edge 8000 GUI](#).

Note

The RAMP Fault Manager lists SNMP traps received from the SBC SWe Edge application of registered Edge 8000 devices. For more information, refer to [Work with Alarm History](#).

Register an SBC Edge Device

Ribbon Application Management Platform (RAMP) manages both hardware-based SBC Edge devices and SBC SWe Edge devices in standalone deployments. It also manages SBC SWe Edge devices in high-availability (HA) deployments.

SBC Edge Registration Prerequisites

On SBC Edge

Manually registering SBC Edge devices is not necessary because the devices automatically register with RAMP after you complete the prerequisite configuration in the SBC Edge GUI. This configuration specifies the RAMP connection parameters for the SBC Edge device.

Using the SBC Edge GUI, configure the RAMP connection parameters for each Edge device you want to register with RAMP. These parameters include the RAMP management address and the management ID of the SBC Edge device. If the SBC Edge device will be part of an SBC SWe Edge HA deployment, include the HA pair name and enable HA on the device. Refer to [Configuring for Ribbon Application Management Platform at Node-level](#) for more information.

On RAMP

To successfully manage SBC Edge devices on RAMP, before the Edge devices attempt to register, you must deploy the EdgeView (EV) service on RAMP and ensure that the RAMP system is registered. To complete RAMP system registration, refer to [System Registration](#). To deploy the EdgeView service, refer to [Deploy Optional Services on RAMP](#).

Managing SBC Edge HA Deployments

When the SBC SWe Edge devices in an HA deployment register with RAMP, the device as part of its registration indicates whether the state of the node is "active" or "standby." The active node should be registered first and then the standby.

If a second node does not register, the first node is still managed as an HA node. RAMP will also allow more than two SBC Edge devices to register using the same HA pair name. However, the EV service raises an [sbcEdgeHANodeCountInvalidNotification](#) alarm when the number of nodes registered with the same HA pair name is a value other than two. For more information on alarms, refer to [SBC Edge Alarms](#).

An SBC Edge HA pair appears as a single entry in the node list on the **Devices** window, under the HA pair name. Click on the HA pair name in the node list to see details on the individual nodes that comprise the HA pair.

Register an EdgeMarc Device

In this section:

- [Register a Standalone Instance of RAMP on EdgeMarc](#)
- [Register a Geographically Redundant RAMP on EdgeMarc](#)

- [View the Registered EdgeMarc device on RAMP](#)

You can manually register EdgeMarc devices on the Ribbon Application Management Platform (RAMP). The first step is to configure RAMP on EdgeMarc by providing RAMP's IP address. On configuring the RAMP IP address on EdgeMarc, log on to the RAMP GUI to view the listed EdgeMarc device.

Prerequisites

- Deploy the EdgeView Service on RAMP. For more information, refer to [Deploy Optional Services on RAMP](#).
- Register ZTP credentials on RAMP.

Register a Standalone Instance of RAMP on EdgeMarc

Perform the following procedure to configure a standalone instance of RAMP on the EdgeMarc GUI.

Start

1. Log on to the EdgeMarc GUI.
2. Navigate to **Admin > Service Configuration**. The Services Configuration window displays.
3. Update the RAMP IP address in the **Set EMPath Management Server** and click **Submit**.

Register a Geographically Redundant RAMP on EdgeMarc

Perform the following to register a Geographically Redundant (GR) RAMP on EdgeMarc:

Start

1. Access the EdgeMarc device through the CLI.
2. Add the IP addresses of both the RAMP instances manually in the `/etc/config/evagent.conf` file.
3. Commit the changes done in the `.conf` file:

```
# cfg_commit
```

4. Restart the ev-agent using `killall evagent`:

An Example:

```
# cat /etc/config/evagent.conf
EDGEVIEW_HOST="10.52.23.12,10.52.22.225"
#cfg_commit
#killall evagent
```

The EdgeMarc device is listed on the RAMP GUI.

View the Registered EdgeMarc device on RAMP

Prerequisites

- RAMP is registered on EdgeMarc.
- Available Super User [privileges](#) for Insight Administration under Core Resources.
- Available Devices and Resource Groups [privileges](#) under Device Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. The registered EdgeMarc device is listed.

Create Clusters for Devices that Dynamically Register with RAMP

A cluster is a group of devices that share the same configuration and work together to perform a common network function. **Ribbon Application Management Platform (RAMP)** manages a cluster as a single device component. Individual devices within a cluster register with **RAMP** dynamically, without manual intervention.

To create a cluster and enable devices to dynamically register with **RAMP**, you first create the cluster on **RAMP**. Then, when you instantiate the devices you want to include in the cluster, you provide them with the cluster ID from the cluster configuration settings, along with the **RAMP** IP address. Once the devices instantiate successfully, they dynamically register to the specified **RAMP** as part of the specified cluster.

RAMP supports clusters providing PSX, SBC, and SLB services. The devices are generally virtualized elements (for example, virtual machines) but in some cases, SBC Core hardware elements can be manually added to a cluster.

Refer to the following topics for information on each type of cluster:

- [Create SBC Clusters](#)
- [Create SLB Clusters](#)
- [Create PSX Clusters](#)

Create SBC Clusters

In this section:

- [OAM Model](#)
- [Direct Single](#)
- [Integrated](#)

To create an SBC Core cluster, you first create the cluster configuration within the **Ribbon Application Management Platform (RAMP)**. During instantiation, the SBC Core devices register with the cluster on **RAMP** using the **RAMP** cluster ID provided through metadata.

In the cluster configuration, you specify management and registration settings for the cluster, such as SNMP parameters and polling intervals. You must also specify which SBC Core devices the cluster will contain and its configuration type. **RAMP** supports three configuration model types for SBC SWE clusters: the OAM-based model, Direct Single model, and Integrated.

OAM Model

In the OAM model, the SBC Core cluster includes an OAM node (or OAM HA pair) that provides a single Operations, Administration, and Maintenance (OAM) interface for the cluster. The OAM node implements the main northbound interface and supports SSH (CLI), NetConf, and REST interfaces. You are allowed to make configuration changes for the cluster on the OAM node, and the OAM replicates those changes to the SBC SWE instances within the cluster.

Note

RAMP supports one OAM node in an active role per cluster.

RAMP maintains the SBC Core configuration archive for the cluster. When you first instantiate the OAM, the OAM obtains the initial cluster configuration (if available) from **RAMP**. You are allowed to configuration changes on the active OAM node. Any configuration changes made on the OAM are saved back to **RAMP** at the same time the configuration replicates to the SBC Core instances within the cluster. Thus **RAMP** maintains the configuration history for the cluster. This enables you to restore the OAM to a previously saved configuration if needed.

Direct Single

The Direct Single model applies only to the SBC Core clusters with a single active SBC Core (either a standalone SBC Core or a 1+1 HA pair). Users make configuration changes on the active SBC Core node to configure the cluster, and the active SBC Core replicates those changes to the standby SBC Core (if any).

Note

For a standalone SBC in a Direct Single cluster, RAMP displays the **Redundancy Type** as HA, since the SBC HA mode is "1to1".

RAMP maintains the SBC Core configuration archive for the cluster. When you first instantiate the active SBC Core, the active SBC Core obtains the initial cluster configuration (if available) from **RAMP**. Any configuration changes made on the active SBC Core are saved back to **RAMP** at the same time the configuration replicates to the standby SBC Core. Similar to the OAM model, you can restore the active SBC Core to a previously saved configuration if needed.

Integrated

From RAMP 24.06 onwards, a new configuration type, **Integrated**, is introduced for the cluster type **SBC Core** and the cluster sub-type **CNe**. The deployment is of (N:1, N=1) where the Active or Standby ISBC pods are available.

Perform the following procedure to create an SBC cluster:

Prerequisites

Establish **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The "Devices" window displays.
3. Click **Add Devices**. The "Add Device" window displays.
4. Select the **Device** as **Cluster** and **Type** as **SBC Core**.
5. Configure the SBC Core cluster parameters based on the following table and click **Save**.

SBC Core Cluster Parameters

Parameter	Length/Range	Description	Mandatory
Device Details			

Parameter	Length/Range	Description	Mandatory
Tenant	N/A	Use this option to implement multi-tenancy. • Root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .	✓
Resource Group	N/A	Select a resource group to add the SBC Core device to an existing resource group. • Root (default) • <any other existing resource group>	
Device	N/A	Select Cluster to create an SBC Core cluster. • Node-Use this option to create a node. • Cluster-Use this option to create a cluster.	
Type	N/A	Select SBC Core as the device type. • SBC Core • PSX • SLB	✓
Name + ID			
Cluster Name	Up to 64 characters	Enter a unique name for the cluster. The cluster name is not case-sensitive. (Allowed characters: Alphanumeric characters, space, hyphen (-), underscore (_), and colon (:))	✓

Parameter	Length/Range	Description	Mandatory
Cluster/VNF Identifier	Up to 64 characters	A Cluster Identifier is a unique key for the cluster. You cannot modify a cluster identifier once you create the cluster. You can enter a value or click Generate ID to have RAMP create an ID for you. Cluster/VNF Identifiers are not case sensitive and can only contain alphanumeric characters and hyphen (and must not start or end with an hyphen). Note A maximum of 64 characters (including additional parameters) are allowed while creating a VNF ID and VNFC ID. For SBC Core instances created using Heat templates, the syntax of the VNFC ID is Stack_Name-Cluster_ID, incorporating the stack name. For example, the VNFC ID becomes SBCSA-5 if the stack name is SBCSA and the Cluster ID is 5. Allowed characters: • Alphanumeric characters and hyphen. • Do not precede or follow the key with a hyphen.	

Parameter	Length/Range	Description	Mandatory
Sub Type	N/A	Select the type of SBC Core cluster: • Integrated: An Integrated SBC Core that manages both signaling and media loads. This is the default value. • Media: A media SBC Core cluster in a distributed deployment. • Signaling: A signaling SBC Core cluster in a distributed deployment. • MRFP: A Media Resource Function Processor (MRFP) cluster. • CNe: Cloud Network Functionality.	✓
Configuration Type	N/A	Select the configuration type: • OAM (default) • Direct Single • Integrated	✓
Performance Management Profile	N/A	If you want to associate an existing Performance Management Profile with the cluster with it, choose it.	
License Profile	N/A	If you want to associate an existing License Profile with the cluster, select it from the drop-down menu.	
Strict Mode	N/A	If you enable this enhanced security option, the device's fingerprint is collected and stored in the DB. RAMP then establishes an SSH connection by validating the device's fingerprint against the fingerprint the device provides while making a connection. Strict Mode is disabled by default.	
SNMP			
SNMP V2 Community	1-25	Enter the SNMPv2 community string to use. SNMP community text strings act as a rudimentary authentication mechanism for SNMPv2 and are used to establish trust between an SNMP manager and an agent. The default value is "hefj6483xhie".	

Parameter	Length/Range	Description	Mandatory
SNMP V3 Security Level	N/A	The SNMP V3 fields presented depend on the security level you choose: • None-(default) No SNMP V3 fields appear. • AuthPriv–All three SNMP V3 fields appear. • AuthNoPriv–SNMP V3 User and SNMP V3 Authentication Protocol appear. • NoAuthNoPriv–Only SNMP V3 User appears. Refer to the following when configuring SNMP V3 options: • SNMP V3 User–Enter the appropriate name of the user, alphanumeric characters only, 5 to 32 characters. • SNMP V3 Authentication Protocol–select MD5 or SHA. • SNMP V3 Privacy Protocol–select AES or DES. The SBC SWe does not support AES-192 and AES-256 bit encryption. Therefore, RAMP sets AES-128 bit encryption as the default.	
Management Client			

Parameter	Length/Range	Description	Mandatory
Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if RAMP has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address. If the Management Client is edited for the cluster, you must edit the RAMP IP address on the device and reboot the device.	
GR Address	IPv4 or IPv6 address format.	This parameter is applicable for a GR RAMP. Lists the primary and secondary (if RAMP has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address. If the Management Client is edited for the cluster, you must edit the RAMP IP address on the device and reboot the device.	

Parameter	Length/Range	Description	Mandatory
Node Registration			
Reachability Polling Interval		Select the duration between checks to determine if the cluster node is up. • 1 minute (default) • 2 minutes • 4 minutes	✓
Registration Notification Interval	1 to 120 minutes	Specify the maximum duration allowed between the initial registration request and the final notification that the node is up. If RAMP does not receive the notification within the set interval, the node transitions to an "unregistered" state and the <code>sonusEmsClusterInstanceUpNotReceivedNotification</code> alarm is raised. The default value is 20 minutes.	✓
Unregistered Node Interval	1 to 180 days	Specify the maximum interval, in days, that a node can be in an unregistered state. After the set interval, RAMP purges the node and raises a <code>sonusEMSClusterNodePurgeNotification</code> alarm. The default value is 7 days.	
Offline Reachability Polling Interval	1 to 240 hours	Specify the maximum interval that a node can fail to respond to reachability polling from RAMP. If the node does not respond within the set interval: • The node transitions to the "unregistered" state. • A <code>sonusEMSClusterNodeDeRegistrationNotification</code> alarm is raised. The default value is 24 hours.	✓
Reachability Polling Interface		Select the interface to use for reachability polling. • SNMP (default) • REST	

Create SLB Clusters

The Ribbon Application Management Platform (RAMP) supports creating a cluster configuration for a standalone SIP-aware Load Balancer (SLB) device or two SLB devices deployed as a 1:1 HA pair. When you instantiate the SLB devices as part of the cluster, they dynamically register with RAMP.

Perform the following procedure to create an SLB cluster:

Prerequisites

Establish **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Cluster** and **Type** as **SLB**.
5. Configure the SLB cluster parameters using the following table and click **Save**.

SLB Cluster Parameters

Parameter	Length/Range	Description	Mandatory
Device Details			
Tenant	N/A	Use this option to implement multi-tenancy. • Root (default) • <any other existing tenants> For more information on multi-tenancy, refer to Configure Multi-Tenancy .	✓
Resource Group	N/A	Select the resource group. • Root (default) • <any other existing resource group>	
Device	N/A	Select Cluster to create a cluster. • Node-Use this option to create a node. • Cluster-Use this option to create a cluster.	✓

Parameter	Length/Range	Description	Mandatory
Type	N/A	Select SLB as the device type. • SBC Core • PSX • SLB	
Name + ID			
Cluster Name	Up to 64 characters.	Enter a unique name for the cluster. The cluster name is not case sensitive. (Allowed characters: Alphanumeric characters, space, hyphen (-), underscore (_), and colon (:))	

Parameter	Length/Range	Description	Mandatory
Cluster/VNF Identifier	Up to 64 characters.	A Cluster Identifier is a unique key for the cluster. Once you create the cluster, you cannot modify a cluster identifier. You can enter a value or click the circular arrows to have RAMP generate an ID for you. Cluster/VNF Identifiers are not case sensitive and can only contain alphanumeric characters and a hyphen (and must not start or end with a hyphen). Note When creating a VNF ID and VNFC ID, a maximum of 64 characters (including additional parameters) are allowed. For SLB instances created using Heat templates, the syntax of the VNFC ID is Stack_Name-Cluster_ID, incorporating the stack name. For example, the VNFC ID becomes SLBSA-5 if the stack name is SLBSA and the Cluster ID is 5. Allowed characters: - Alphanumeric characters and hyphen. - Do not precede or follow the key with a hyphen.	✓
Performance Management Profile	N/A	If you want to associate an existing Performance Management Profile with the cluster with it, choose it.	
License Profile	N/A	If you want to associate an existing License Profile with the cluster, select it from the drop-down menu	

Parameter	Length/Range	Description	Mandatory
Strict Mode	N/A	If you enable this enhanced security option, the device's fingerprint is collected and stored in the DB. RAMP then establishes an SSH connection by validating the device's fingerprint against the fingerprint the device provides while making a connection. Strict Mode is disabled by default.	
SNMP			
SNMP V2 Community	1-25	Enter the SNMPv2 community string to use. SNMP community text strings act as a rudimentary authentication mechanism for SNMPv2 and are used to establish trust between an SNMP manager and an agent. The default value is "hefj6483xhie".	

Parameter	Length/Range	Description	Mandatory
SNMP V3 Security Level	N/A	The SNMP V3 fields presented depend on the security level you choose: • None—(default) No SNMP V3 fields appear. • AuthPriv—All three SNMP V3 fields appear. • AuthNoPriv—SNMP V3 User and SNMP V3 Authentication Protocol appear. • NoAuthNoPriv—Only SNMP V3 User appears. Use this field to configure SNMP V3 options: • SNMP V3 User—Enter the appropriate name of the user, alphanumeric characters only, 5 to 32 characters. • SNMP V3 Authentication Protocol—select MD5 or SHA. • SNMP V3 Privacy Protocol—select AES or DES. Note The SLB does not support AES-192 and AES-256 bit encryption. Therefore, RAMP sets AES-128 bit encryption as the default.	
Management Client			

Parameter	Length/Range	Description	Mandatory
Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if RAMP has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address. If the Management Client is edited for the cluster, you must edit the RAMP IP address on the device and reboot the device.	
GR Address	IPv4 or IPv6 address format.	This parameter is applicable for a GR RAMP. Lists the primary and secondary (if RAMP has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address. If the Management Client is edited for the cluster, you must edit the RAMP IP address on the device and reboot the device.	

Parameter	Length/Range	Description	Mandatory
Node Registration			
Reachability Polling Interval	N/A	Select the duration between checks to determine if the cluster node is up. • 1 minute (default) • 2 minutes • 4 minutes	✓
Registration Notification Interval	1 to 120 minutes.	Specify the maximum duration allowed between the initial registration request and the final notification that the node is up. If RAMP does not receive the notification within the set interval, the node transitions to an "unregistered" state and the <code>sonusEmsClusterInstanceUpNotReceivedNotification</code> alarm is raised. The default value is 20 minutes.	✓
Unregistered Node Interval	1 to 180 days.	Specify the maximum interval, in days, that a node can be in an unregistered state. After the set interval, RAMP purges the node and raises a <code>sonusEMSClusterNodePurgeNotification</code> alarm. The default value is 7 days.	
Offline Reachability Polling Interval	1 to 240 hours.	Specify the maximum interval that a node can fail to respond to reachability polling from RAMP. If the node does not respond within the set interval: • The node transitions to the "unregistered" state. • A <code>sonusEMSClusterNodeDeRegistrationNotification</code> alarm is raised. The default value is 24 hours.	✓
Reachability Polling Interface	N/A	Select the interface to use for reachability polling. • SNMP (default) • REST	

Create PSX Clusters

To create a PSX cluster, first create the cluster configuration within the Ribbon Application Management Platform (RAMP). During instantiation, the PSX devices register with the cluster on RAMP using the RAMP cluster ID provided through metadata.

In a cluster configuration, specify the cluster's management and registration settings, such as SNMP parameters and polling intervals. For PSX clusters, you must also specify whether the cluster is Primary or Replica.

From PSX 15.x onwards, a cluster supports multiple primary PSX nodes and one provisioning primary PSX node in a primary cluster. The provisioning primary PSX node is the first to register to a cluster on RAMP.

Perform the following procedure to create a PSX cluster:

Prerequisites

- Establish Read and write permissions under **PSX Management**.
- Establish **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. Click **Add Devices**. The **Add Device** window displays.
4. Select the **Device** as **Cluster** and **Type** as **PSX**.
5. Configure the PSX cluster parameters using the following table and click **Save**.

PSX Cluster Parameters

Parameter	Length/Range	Description	Mandatory
Device Details			
Tenant	N/A	Use this option to implement multi-tenancy. • Root (default) • <any other existing resource group> For more information on multi-tenancy, refer to Configure Multi-Tenancy .	
Resource Group	N/A	Select a resource group to add the PSX device to an existing resource group. • Root (default) • <any other existing resource group>	
Device	N/A	Select Cluster to create a PSX cluster. • Node • Cluster	

Parameter	Length/Range	Description	Mandatory
Type	N/A	Select PSX as the device type. • SBC Core • PSX • SLB	✓
Name + ID			
Cluster Name	Up to 64 characters. Alphanumeric characters, space, hyphen (-), underscore (_), and colon (:).	Enter a unique name for the cluster. The cluster name is not case-sensitive.	✓
Cluster/VNF Identifier	Up to 64 characters. • Alphanumeric characters and hyphen. • Do not precede or follow the key with a hyphen.	A Cluster Identifier is a unique key for the cluster. Once you create the cluster, you cannot modify a cluster identifier. You can enter a value or click the circular arrows to have RAMP create an ID for you. Cluster/VNF Identifiers are not case sensitive. Note The VNF ID and VNFC ID are limited to a maximum of 64 characters of length. If a VNF ID includes additional parameters, ensure that the total number of characters (VNFC ID plus additional parameters) does not exceed 64.	✓
Sub Type	N/A	Select whether the PSX is a primary node or a replica node. • Primary PSX: devices can be grouped together. Each primary has its own Postgres database, but data between primary PSX devices is synced. • A replica PSX device refers to its primary.	✓

Parameter	Length/Range	Description	Mandatory
Performance Management Profile	N/A	If you want to associate an existing Performance Management Profile with the cluster with it, choose it.	
License Profile	N/A	If you want to associate an existing License Profile with the cluster, select it from the drop-down menu.	
Strict Mode	N/A	If you enable this enhanced security option, the device's fingerprint is collected and stored in the DB. RAMP then establishes an SSH connection by validating the device's fingerprint against the fingerprint the device provides while making a connection. Strict Mode is disabled by default.	
SNMP			
SNMP V2 Community	1-25	Enter the SNMPv2 community string to use. SNMP community text strings act as a rudimentary authentication mechanism for SNMPv2 and are used to establish trust between an SNMP manager and an agent. The default value is "hefj6483xhie".	✓

Parameter	Length/Range	Description	Mandatory
SNMP V3 Security Level	N/A	The SNMP V3 fields presented depend on the security level you choose: • None– (default) No SNMP V3 fields appear. • AuthPriv–All three SNMP V3 fields appear. • AuthNoPriv–SNMP V3 User and SNMP V3 Authentication Protocol appear. • NoAuthNoPriv–Only SNMP V3 User appears. Refer to the following when configuring SNMP V3 options: • SNMP V3 User – Enter the appropriate name of the user, alphanumeric characters only, 5 to 32 characters. • SNMP V3 Authentication Protocol – select MD5 or SHA. • SNMP V3 Privacy Protocol – select AES or DES.	
Management Client			

Parameter	Length/Range	Description	Mandatory
Address	IPv4 or IPv6 address format.	Lists the primary and secondary (if RAMP has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. Discover the node after updating the Management Client Address. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address. If the Management Client is edited for the cluster, you must edit the RAMP IP address on the device and reboot the device.	
GR Address	IPv4 or IPv6 address format.	This parameter is applicable for a GR RAMP. Lists the primary and secondary (if RAMP has a secondary interface) IP addresses of the current standby RAMP instance. You are allowed to edit the entry even after registering the node. By default, the secondary IP address is selected if the RAMP has a secondary interface. Note Ensure the networks are reachable before editing the IP address. If the Management Client is edited for the cluster, you must edit the RAMP IP address on the device and reboot the device.	

Parameter	Length/Range	Description	Mandatory
Node Registration			
Reachability Polling Interval	N/A	Select the duration between checks to determine if the cluster node is up. • 1 minute (default) • 2 minutes • 4 minutes	✓
Registration Notification Interval	1-120	Specify the maximum duration allowed, in minutes, between the initial registration request and the final notification that the node is up. If RAMP does not receive the notification within the set interval, the node transitions to an "unregistered" state and the <code>sonusEmsClusterInstanceUpNotReceivedNotification</code> alarm is raised. The default value is 20 minutes.	✓
Unregistered Node Interval	1-180	Specify the maximum interval, in days, that a node can be in an unregistered state. After the set interval, RAMP purges the node and raises a <code>sonusEMSClusterNodePurgeNotification</code> alarm. The default value is 7 days.	✓
Offline Reachability Polling Interval	1-240	Specify the maximum interval, in hours, that a node can fail to respond to reachability polling from RAMP. If the node does not respond within the set interval: • The node transitions to the "unregistered" state. • A <code>sonusEMSClusterNodeDeRegistrationNotification</code> alarm is raised. The default value is 24 hours.	✓
Rest Reachability Polling Interface	N/A	Select the interface to use for reachability polling. • SNMP (default) • REST	

Edit RAMP Device Registration

Ribbon Application Management Platform (RAMP) automatically registers itself as a managed device so that it can monitor its own basic system health.

For a RAMP standalone instance, the instance registers after installation and an entry automatically appears for it in the node list as "localhost". For a RAMP geographically redundant (GR) system, the instances register after you configure GR parameters so that the source RAMP shows two entries: one for the source RAMP and another for the target RAMP. The node list reflects the names entered for the nodes during GR configuration.

After RAMP registers, you can manually update its registration settings. To improve system security, Ribbon recommends that you change the default values of the Agent password and SNMP strings for the localhost.

Note

Re-discover RAMP after changing the Agent password, SNMP strings, or the Reachability Polling interval. To discover nodes, refer to [How to Rediscover the localhost](#).

Prerequisites

- The device is up and running.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. In the **Nodes** list row for the localhost (standalone or GR) you want to edit, select the pencil icon under **Action** to open the edit page. Note that some parameters can no longer be changed. Options that are no longer editable appear as read-only text on the Edit window.
4. Use the following table to edit the parameters as needed and click **Save**.
5. To re-discover a localhost (standalone or GR) after making changes, in the **Nodes** list row for the localhost, click the ellipses (...) menu under **Action** and select **Discover**.

RAMP Parameters

Parameter	Description	Length/ Range
Node Information		
Name	Enter a name for the RAMP system to change from localhost. The default is "localhost".	N/A
Node IP		

Parameter	Description	Length/ Range
Primary IP	Enter the primary IP address of RAMP.	N/A
Secondary IP	Enter the secondary IP address of RAMP.	N/A
Interfaces Agent:		
Username	Enter a username for the Agent. The default is "admin".	N/A
Password	Enter a password for the Agent.	N/A
SNMP Configuration		
SNMP Read Community	Enter the SNMP Read Community String. Ribbon strongly recommends changing the default SNMP Community strings for security reasons.	N/A
Port Number	Enter the port number to which to send SNMP queries. The default value is "161".	N/A
SNMPv3 Security Level	The parameter is applicable only for SNMPv3. Select the type of security model to apply to SNMP connections: • None (Default) – no security. • AuthPriv – authentication is required, and messages are encrypted. • AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. • NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private. The default value is "None".	• No ne • AuthPriv • AuthNoPriv • NoAuthNoPriv
SNMPv3 User	Specifies the name of the SNMPv3 User name. NOTE: The parameter is applicable only if Security Level is set to one of the following: • AuthPriv • AuthNoPriv • NoAuthNoPriv	5 to 32 alphanumeric characters

Parameter	Description	Length/Range
SNMPv3 Authentication Protocol	Select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol to enable private interactions over secure channels. The options are: • MD5 • SHA NOTE: • If you register a JTIC enabled SBC on a JTIC enabled RAMP, then MD5 is not supported. • This parameter is applicable only if Security Level is set to AuthPriv or AuthNoPriv.	N/A
SNMPv3 Auth PassPhrase	This is the SNMPv3 authorization password. NOTE: This parameter is applicable only if Security Level is set to AuthPriv or AuthNoPriv.	
SNMPv3 Privacy Protocol	Specifies the SNMPv3 privacy options: • AES • DES Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. NOTE: If you register a JTIC enabled SBC on a JTIC enabled RAMP, then DES is not supported. NOTE: This parameter is applicable only if Security Level is set to AuthPriv.	N/A
SNMPv3 Priv PassPhrase	This is the SNMPv3 privacy password. NOTE: This parameter is applicable only if Security Level is set to AuthPriv or AuthNoPriv.	N/A
Reachability		
Polling Interval	Select how often RAMP verifies that the node is reachable. • None • 1 Minute (default) • 2 Minutes • 4 Minutes	N/A
Interface	Select the interface to use for reachability polling. • SNMP	N/A

Manage Registered Nodes

Additional articles:

- [View and Edit Node Registration Parameters](#)
- [View Node Information and Status](#)
- [View Node Inventory Details](#)
- [Discover Nodes](#)
- [Unregister Nodes](#)
- [Delete Nodes](#)
- [Manage SBC Edge Devices](#)
 - [View Voice Quality Reports for SBC Edge Devices](#)
 - [View Call Data Charts for SBC Edge Devices](#)
- [Manage EdgeMarc Devices](#)
 - [Back up and Restore EdgeMarc Devices](#)
 - [Configure Devices on EdgeMarc](#)
 - [Manage EdgeMarc Automated Provisioning](#)
 - [Manage EdgeMarc Profiles](#)
 - [Policy Parameters for EdgeMarc Devices](#)
 - [Upgrade Firmware for EdgeMarc Devices](#)
 - [View Attached Devices for EdgeMarc](#)
 - [View Call Charts for EdgeMarc Devices](#)
- [Generate or Change Passwords](#)
 - [Generate Passwords for Cloud-Based SBC or SLB Devices](#)
 - [Generate Passwords for PSX Devices](#)
 - [Change Password for EdgeMarc Devices](#)
- [Job Status](#)

The Ribbon Application Management Platform (RAMP) Device Management services provide a range of software and network management functions for both hardware-based and virtualized Ribbon devices. On RAMP, managed devices include both individual nodes and clusters.

After they register, you can manage devices by navigating to **DEVICE MANAGEMENT > Devices**.

The **Devices** window opens with the **Nodes** tab in view, listing all of the nodes that are currently registered with RAMP. Each node list entry provides a summary of information on a particular node, including its general status. Click on the node name to drill down to more details on the selected node. The options under **Action** enable you to perform a variety of actions on the corresponding node. The options that are available depend on the type of node and its current status.

The topics in this section describe specific ways you can work with nodes on RAMP.

Prerequisites for Managing Registered Devices

You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

View and Edit Node Registration Parameters

Ribbon Application Management Platform (RAMP) supports editing some registration parameters of devices that are manually registered. Not all parameters are editable for registered devices. Options that are no longer editable appear as read-only text on the Edit window.

Prerequisite

- The device is up and running.
- Available **User privileges** for **GUI** under **Core Resources**.
- Available **Devices** and **Resource Groups privileges** under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the row for the device to edit, select the pencil icon under **Action** to open an edit device page. Note that you can no longer change some parameters.
4. Refer to the Parameter table on one of the following pages, based on the device you want to edit:

Device	Procedure
C3 G9EMS device	Register a C3 or G9EMS Devices
C20	Register a C20 Device
DELL	Register a DELL Device
DSC	Register a DSC Device
DSI	Register a DSI Device
G5	Register a G5 Device
G6MM	Register a G6MM Device
GMS	Register a GMS Device
GSX	Register a GSX Device
IDH	Register an IDH Device
L2MGR	Register an L2MGR Device
PSX	Register a PSX Device
RAMP	Edit RAMP Device Registration
SBC Core	Register an SBC Core Device
SLB	Register an SLB Device
SGX	Register an SGX Device

Device	Procedure
STI	Register an STI Device.

5. Click **Save** to apply any changes.

View Node Information and Status

After you register devices with Ribbon Application Management Platform (RAMP), they are listed on the **Devices** page that is provided by RAMP's Device Management service. The **Node** tab on the **Devices** page contains a list of all registered nodes. From this list, work with specific nodes to obtain different types of information and perform actions on the node. The types of information and actions available differ significantly based on the type, deployment mode, and current state of the device. Additionally, RAMP provides general node information and status for all managed nodes.

General Node Information and Status

RAMP provides an **Overview** tab for each of managed device. Review the **Overview** tab for a summary of key registration settings, such as the current configuration of interfaces, SNMP, and IP addresses. The **Overview** tab also reports current status information such as the device's registration status and the date and time when the node was last discovered by RAMP.

For PSX 15.x and above, a new field, **Role** is included. This depicts if the PSX is a provisioning primary or primary. For the PSX replica, a new field, **Primary Cluster ID**, is included in the **Overview** tab because the replica is associated to the primary PSX cluster instead of the primary PSX node.

For EdgeMarc devices, the **Node Status** tab displays information on the **SIP Server Status**, **LAN/WAN**, **T1**, **ARP Cache Status**, and **Policy Compliance**.

For SBC 1000/2000 devices, the **Overview** tab displays information on the **SBA Configuration**.

Use the following procedure to see general information for a selected device.

Prerequisite

Obtain permission/access to Devices under Device Management of [User Privileges in RAMP](#).

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. In the **Nodes** list, click on the **Node Name** for the device to open the **Overview** tab which contains status and details for the selected device.

The information on the **Overview** tab is not directly editable. However, as a convenience when you are viewing details for the device, RAMP provides a **Select Action** menu to initiate actions for the node (such as Configure, Edit, Discover, Delete, and so on) similar to those that appear under **Actions** in the **Devices** window.

View Node Inventory Details

The Ribbon Application Management Platform (RAMP) regularly retrieves inventory information for each SBC Core, SBC Edge, DSC, and SLB device and provides the node data of these device types. The inventory contents differ depending on the specific type of device and can include information such as hardware, software, firmware, resources, redundancy, database, and revision history.

For SBC Core, SLB, and DSC devices, the RAMP collects inventory information in the following categories applicable to the specific node:

- Node Info
- Hardware Info
- Software Info
- Slot Info
- Power Supply Unit

For SBC Edge devices, RAMP collects inventory information in the following categories applicable to the specific node:

- Port Licenses
- Feature Licenses
- Node Modules
- Ports

RAMP provides only feature license information for virtualized SBC SWe Edge devices. Only the licensed feature licenses are displayed.

Use the following procedure to see inventory information for a selected device.

Prerequisite

You must have **Devices**, **Resource Groups**, and **Inventory Reports** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. In the **Nodes** list, click on the **Node Name** of a device to view its details.
4. Click on the **Inventory** tab to see the inventory information for the selected device.

Discover Nodes

For devices that you manage with Ribbon Application Management Platform (RAMP), node discovery enables RAMP to gather information on the current state of the device. A node is discovered automatically when you register it with RAMP. When you make changes to the device, such as an upgrade, then you can discover a node manually.

Prerequisites

- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window opens.
3. In the **Nodes** list row for the device you want to discover, click the ellipses (...) menu under **Action** and select **Discover**. RAMP displays a success message when it completes discovery.

Note

For SBC Edge, node **Discovery** is supported only for SBC 1000/2000 devices.

Unregister Nodes

You can unregister manually registered devices from Ribbon Application Management Platform (RAMP) to stop managing them using RAMP. Nodes that register dynamically must be in the register-offline state before they can be unregistered.

Automatically registered SBC Edge devices cannot be unregistered. However, registered SBC Edge devices can be deleted when they are offline.

For PSX 15.x and above, the provisioning primary PSX should be the last node in the cluster to be unregistered. Non-provisioning primary and replica nodes can be unregistered in any order. Once all the non-provisioning primary and replica nodes are unregistered, the provisioning primary can be unregistered.

Prerequisites

- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the Ribbon Application Management Platform GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window opens.
3. In the **Nodes** list row for the device you want to unregister, click the ellipses (...) menu under **Action** and select **Unregister**.

Delete Nodes

You can free up Ribbon Application Management Platform (RAMP) memory by deleting any devices that are no longer registered on RAMP.

When you delete a device, RAMP removes all information related to the device. Manually and dynamically registered devices must be unregistered before deleting.

Prerequisites

- Ensure that device is in unregistered.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the **Nodes** list row for the device you want to delete, click the delete icon under **Action**.
4. Confirm the deletion when prompted.

Manage SBC Edge Devices

Additional articles:

- [View Voice Quality Reports for SBC Edge Devices](#)
- [View Call Data Charts for SBC Edge Devices](#)

The Ribbon Application Management Platform (RAMP) supports viewing Voice Quality Reports (VQR) for SBC Edge devices and call data in chart format for a selected SBC SWe Edge device.

RAMP does not display call data in chart format for SBC 1000/SBC 2000 devices.

View Voice Quality Reports for SBC Edge Devices

You can view Voice Quality Reports (VQR) for SBC Edge devices. VQR reports include details such as the time of a call, source, destination, jitter, and latency that can assist in troubleshooting a call.

For more information on VQR, refer to [Voice Quality Reporting to Ribbon Application Management Platform](#).

Prerequisites

- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. In the **Nodes** list, click on the **Node Name** of an SBC Edge device to view its details.
4. Click the **Call Log** tab.

View Call Data Charts for SBC Edge Devices

You can view call data in chart format for a selected SBC SWe Edge device on Ribbon Application Management Platform (RAMP).

The chart shows the maximum number of concurrent sessions for every 60 minutes interval in the last 6/12/18/24 hours which includes:

- SIP sessions
- SIP sessions with Transcode Services
- SIPREC sessions
- DSPC sessions

RAMP does not display call data in chart format for SBC 1000/SBC 2000 devices.

Prerequisites

- You must have Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. In the **Nodes** list, click on the **Node Name** of an SBC Edge device to view its details.

4. Click the **Charts** tab.

Manage EdgeMarc Devices

Additional articles:

- [Back up and Restore EdgeMarc Devices](#)
- [Configure Devices on EdgeMarc](#)
- [Manage EdgeMarc Automated Provisioning](#)
- [Manage EdgeMarc Profiles](#)
- [Policy Parameters for EdgeMarc Devices](#)
- [Upgrade Firmware for EdgeMarc Devices](#)
- [View Attached Devices for EdgeMarc](#)
- [View Call Charts for EdgeMarc Devices](#)

The Ribbon Application Management Platform (RAMP) allows you to view call data charts, attached devices, and manage profiles for a selected EdgeMarc device. You can also upgrade the firmware for a particular EdgeMarc device.

Back up and Restore EdgeMarc Devices

Ribbon Application Management Platform (RAMP) supports backing up and restoring EdgeMarc devices, and acts as a repository for your device backup. The system backup files contain configuration data. You can retrieve the system files from the servers of the managed device. The generated files are stored in the RAMP database.

In this section:

- [Back up EdgeMarc Devices](#)
- [Restore EdgeMarc Devices](#)
- [Reboot EdgeMarc Devices](#)
- [View and Compare Backup Files for EdgeMarc Devices](#)

Back up EdgeMarc Devices

In this section:

- [Backup EdgeMarc Devices](#)
- [Job Status](#)

Use the following procedure to back up your EdgeMarc devices. The Ribbon Application Management Platform (RAMP) serves as the repository for the device backup files, which contain configuration data and other binary files.

You can schedule a backup based on your backup strategy.

Prerequisites

- **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices, Resource Groups, and Job Status** [privileges](#) under **Device Management**.

Backup EdgeMarc Devices**Start**

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Devices**.
3. Select the EdgeMarc device to backup.
4. From the **Bulk Actions** menu, select **Backup**. The **Backup** window displays.
5. The **Included Devices** pane lists the configured EdgeMarc devices on RAMP.
6. Update the **Backup Name** and **Frequency** to take a backup and click **Save**. Refer to the following table for parameter descriptions.

Parameters

Parameter	Description	Length/Range
Backup Name	Provide a name for the backup you want to take.	0-64 alphanumeric characters.
Frequency		
One Time Only		
Perform Now	The default value is One Time Only, Perform Now .	
Perform Later	Select this option to take a backup by providing the Date .	
Hourly	Select the time (in minutes) after every hour and the start and end date to schedule the backup.	0-55 Minutes after the hour.
Daily	Select the time, start and end dates to schedule the backup. The format is hh:mm:ss. h: hours m: minutes s: seconds	00:00:00-23:59:59
Weekly	Select the: • day • time • start and end dates to schedule the backup.	• Monday-Sunday • 00:00:00-23:59:59

Parameter	Description	Length/Range
Monthly	Select the: • day • time • start and end dates to schedule the backup.	• 1-30 or 1-31, depending upon the calendar month. • 00:00:00-23:59:59
Comments	Enter comments or a note for your reference.	
Notification	Enable this option to receive in-app status notifications when a particular action is completed. Note You can view this option only when Notification Service is deployed on the RAMP.	

Job Status

Perform the following procedure to view the status of the devices after a backup:

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Job Status**. The **Job Status** window displays.
3. In the **Type** column, select the row to view the status.
4. Hover the mouse over the status bar to view the status of each job.

Restore EdgeMarc Devices

The Ribbon Application Management Platform (RAMP) supports restoring EdgeMarc devices using backup files stored in RAMP.

You can schedule to restore from the latest backup at your convenience.

Prerequisites

- **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices, Resource Groups, and Job Status** [privileges](#) under **Device Management**.
- Restore action picks up the latest backup configuration to restore. The Backup action must have been executed at least once previously. For more information, refer [Back up EdgeMarc Devices](#).

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Devices**.

3. Select the EdgeMarc device to restore from a backup.
4. From the **Bulk Actions** menu, select **Restore**. The **Restore** window displays.
5. The **Included Devices** pane lists the configured EdgeMarc devices on RAMP.
6. Use the following table to update the **Frequency** to restore from the backup and click **Save**.

Parameters

Parameter	Description	Length/Range
Frequency		
One Time Only		
Perform Now	The default value is One Time Only, Perform Now .	
Perform Later	Select this option to take a restore by providing: • Date • Time	• 1-30 or 1-31, depending upon the calendar month. • 00:00:00-23:59:59
Comments	Enter comments or a note for your reference.	
Notification	Enable this option to receive in-app notification about the status when the particular action is completed. Note This option is only available when the Notification Service is deployed on the RAMP.	

Reboot EdgeMarc Devices

In this section:

- [Reboot EdgeMarc Devices](#)
- [Job Status](#)

The Ribbon Application Management Platform (RAMP) supports Rebooting EdgeMarc devices.

Prerequisites

- **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices**, **Resource Groups**, and **Job Status** [privileges](#) under **Device Management**.

Reboot EdgeMarc Devices

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Devices**.
3. Select the EdgeMarc device to reboot.
4. From the **Bulk Actions** menu, select **Reboot**. The **Reboot** window displays.
5. The **Included Devices** pane lists the configured EdgeMarc devices on RAMP.
6. Use the following table to update the **Name** and **Frequency** to reboot and click **Save**.

Parameters

Parameter	Description	Length/Range
Frequency		
One Time Only		
Perform Now	The default value is One Time Only , Perform Now .	
Perform Later	Select this option to reboot by providing the Date .	
Hourly	Select the time (in minutes) after every hour and the start and end date to schedule the reboot.	0-55 Minutes after the hour.
Daily	Select the time, start and end dates to schedule the reboot. The format is hh:mm:ss. h: hours m: minutes s: seconds	00:00:00-23:59:59
Weekly	Select the: • day • time • start and end dates to schedule the reboot.	• Monday-Sunday • 00:00:00-23:59:59

Parameter	Description	Length/Range
Monthly	Select the: • day • time • start and end dates to schedule the reboot.	• 1-30 or 1-31, depending upon the calendar month. • 00:00:00-23:59:59
Comments	Enter comments or a note for your reference.	
Notification	Enable this option to receive in-app notification about the status when the particular action is completed. NOTE: You can view this option only when Notification Service is deployed on the RAMP.	

Job Status

Perform the following procedure to view the status of the devices after a reboot:

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Job Status**. The **Job Status** window displays.
3. In the **Type** column, select the row to view the status.
4. Hover the mouse over the status bar. The status of each job is displayed.

View and Compare Backup Files for EdgeMarc Devices

The Ribbon Application Management Platform (RAMP) supports backing up EdgeMarc devices, and acts as a repository for your device backup. The backup files are stored on the RAMP database thereby enabling you to view, compare, and restore a copy of the backup.

Prerequisites

- Posses **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- Posses **Devices, Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Devices**. The **Devices** window displays.
3. In the nodes list, click on the **Node Name** of an EdgeMarc device to view its details.
4. Click the **Backup** tab. The Backup window displays.
5. **Select backup to view its content**. The contents of the backup file are displayed.
6. Click **Compare** to compare two different backup files. The difference between the selected backup files are displayed.
7. Click **Restore** to restore the backup.

Configure Devices on EdgeMarc

In this section:

- [Configure Devices on EdgeMarc](#)
- [Job Status](#)

The Ribbon Application Management Platform (RAMP) supports Configuring devices on EdgeMarc.

Prerequisites

- **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices**, **Resource Groups**, and **Job Status** [privileges](#) under **Device Management**.

Configure Devices on EdgeMarc

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Devices**.
3. Select the EdgeMarc device to Configure.
4. From the **Bulk Actions** menu, select **Configure Device**. The **Configure Device** window displays.
5. The **Included Devices** pane lists the configured EdgeMarc devices on RAMP.
6. Use the following table to update the parameters then click **Save**.

Parameters

Parameter	Description	Length/Range
Configuration File	Drag and drop or browse for the file to upload the configuration file.	
Configuration Parameters		
Network Settings		
EdgeMarc network settings		
The first checkbox is to Push, and the second checkbox is to Enable/Disable the parameters.		
LAN IPv4 Address	Provide the IPv4 address.	Provide a valid IPv4 address.
Prefix	1-32.	Provide the prefix.
LAN IPv6 Address		Provide the IPv6 address.
Prefix	1-128	Select the prefix.

Parameter	Description	Length/Range
WAN Interface IPv4 settings		Select the type of IP address. The options are: • Static IP • DHCP If you select Static IP: Provide the following details. • WAN IP Address: Provide the WAN IP Address. • Prefix: Select a value from 1-32. • WAN Gateway: Provide the WAN gateway.
WAN Interface IPv6 settings	N/A	Select one of the following: • Disable: Disables the WAN interface IPv6 settings. • Static IP: Provide the WAN IPv6 address, prefix (1-128), and the WAN gateway. • DHCP
Manually set DNS	N/A	Provide the following details: • WAN DNS Primary • WAN DNS Secondary
Enable SNTP	N/A	Provide the Time Server. For example, time.nist.gov.
Enable DHCP Server	N/A	Provide the following: • IP Address Range: If you have a range of IP addresses, provide the first IP address and the last IP address. • DHCP Server - Option 42: Provide a valid IPv4 or IPv6 address. • DHCP Server - Option 66: Provide a valid IPv4 or IPv6 address.
Secondary WAN Interface IPv4 settings	N/A	Select one of the following: • Disable Secondary WAN. • Static IP: Provide the WAN IPv4 address, prefix (1-32), and the WAN gateway. • DHCP.

Parameter	Description	Length/Range
Secondary WAN Interface IPv6 settings	N/A	Select one of the following: • Disable Secondary WAN. • Static IP: Provide the WAN IPv6 address, prefix (1-128), and the WAN gateway. • DHCP.
Manually set DNS for Secondary WAN	N/A	Provide the following: • Secondary WAN - DNS Primary • Secondary WAN - DNS Secondary
Security Settings		
Security Page	Select any of the following: • Allow SSH access through firewall • Allow HTTP access through firewall • Allow HTTPS access through firewall • Allow SNMP access through firewall There is no default value.	N/A
Admin/Service Config Settings		
Settings related to Admin/Service Config	Select any of the following: • Enable SNMPv1: ◦ Set SNMPv1 Read - Only Community: <TBD> ◦ Set SNMPv1 Host: Provide a valid IPv4 or IPv6 address. • Enable Remote System Logging: Provide a valid IPv4 or IPv6 address. • Enable MOS Scoring: Set the MOS scoring. The valid range is 0-5. • Enable Analytics: Set the Analytics Timeout. the valid range is 2-1666666. • Enable System Monitor: Enable this option to monitor the system.	N/A

Parameter	Description	Length/Range
Trusted Hosts Settings	Trusted Hosts allows a user to define a list of hosts or networks that are allowed to access this system via management protocols.	
Enable Trusted Hosts	Select the Checkbox to define a list of hosts that are allowed to access the system through the management protocols. Add Trusted Hosts: Provide the following information. Set IP Addresses for Trusted Hosts: Provide a valid IPv4 or IPv6 address. Port: Provide a port number from 1-32.	N/A
VOIP Settings		
SIP protocol settings		
SIP Server Name	Provide a valid IPv4 or IPv6 address.	N/A
SIP Server Port	Select the checkbox to enter the SIP Server Port.	0-32768
SIP Server Transport	Select one of the following transport types: • Pass Through • UDP • TCP • TLS	N/A
Use Custom Domain		
SIP Server Domain	Provide a valid IPv4 or IPv6 address.	
Enable Multi-Homed Outbound Proxy Mode:		
Client UDP Listening ports	Choose the port from the options.	0-32768
Enable LAN device UA name pass-through		
Enable Transparent Proxy mode		
Survivability Settings		

Parameter	Description	Length/Range
Settings related to Survivability Page	Provide or select the following parameters: • Enable Keepalives • Error codes: Provide a valid error code. • Rate - Pacing behaviour: Select one of the following ◦ Configured Value: provide the configured value. • Rate-Pacing interval: Provide the rate pacing interval. The valid range is 1-999999. The default value is 1800. ◦ None (Rate-Pacing is disabled). ◦ Soft-Switch/IP PBX Provided Value. • Enable SIP server Redundancy: • Enable Phone Expires Override: Provide a value. The valid range is 0-999999. The default value is 20. • Monitor SIP Messages.	
Frequency		
One Time Only		
Perform Now	The default value is One Time Only, Perform Now.	N/A
Perform Later	Select this option to schedule the config push for a later time by selecting a specific date and time.	N/A
Comments	Enter comments or a note for your reference.	N/A

Parameter	Description	Length/Range
Notification	Enable this option to receive in-app notification about the status when the particular action is completed. You can view this option only when Notification Service is deployed on the RAMP.	N/A

Job Status

Perform the following procedure to view the status of the devices after configuring:

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Job Status**. The **Job Status** window displays.
3. In the **Type** column, select the row to view the status.
4. Hover the mouse over the status bar. The status of each job is displayed.

Manage EdgeMarc Automated Provisioning

In this section:

- [Auto-Provision EdgeMarc Devices](#)
- [Auto-Provisioning Policy for EdgeMarc Devices](#)
- [Provisioning Status of EdgeMarc Devices](#)

Auto-Provision EdgeMarc Devices

Use the RAMP EdgeView service to set EdgeMarc devices for auto provisioning. This procedure informs the ZTP that if there is a registration request from a particular EdgeMarc device, then ZTP must redirect the EdgeMarc to the particular RAMP.

Prerequisites

- **Resource Groups** and **Provisioning Policy privileges** under **Device Management**.
- RAMP is registered with ZTP.

Use this procedure to auto-provision an EdgeMarc device.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Auto-Provisioning**. The "Auto-Provisioning" window displays.
3. In the **Add Devices to Auto-Provision** pane, select either **Enter LAN MAC Address** or **Bulk Add LAN MAC Address**.

Ribbon recommends using the Bulk Add option to provision more than 10 devices.

- a. If you select **Enter LAN MAC Address**, enter the MAC addresses for the LAN one after another and click **Verify**.
- b. Use **Bulk Add LAN MAC Address** if you want to provision more than 10 devices.
 - i. Click **Upload** file. The "Upload File" dialog displays.
 - ii. Click **Browse for file**.

Note

Ensure this file contains MAC addresses separated by commas or new lines.

- iii. Navigate to select the folder and file.
- iv. Click **Open**. The file is uploaded.
- v. Alternatively, you can drag and drop the files on to the upload file dialog.
- vi. Click **Verify**. Wait for the upload success message to display.
4. In the **Select devices from below to be auto-provisioned** pane, select the EdgeMarc devices you want to auto-provision.
5. In the **Select Policy to be Applied to the devices** pane, select the policy to apply. To add a new provisioning policy, refer to [Auto-Provisioning Policy for EdgeMarc Devices](#).
6. Click **Auto-Provision**.

Auto-Provisioning Policy for EdgeMarc Devices

The Ribbon Application Management (RAMP) ensures that EdgeMarc devices are auto-provisioned with the desired configuration and firmware version.

Prerequisites

- **Resource Groups, Provisioning Policy, and Firmware Repository privileges** under **Device Management** are set
- **Tenant administration privileges** under **Authentication & Authorization** are set

Add a Policy

Perform the following procedure to add a policy.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Provisioning Policy**. The **Provisioning Policy** window displays.
3. Click **+ Add Policy**. The **Add Policy** window displays.
4. Specify the policy parameters. For more information, refer to [Policy Parameters for EdgeMarc Devices](#).
5. Click **Save**.

Provisioning Status of EdgeMarc Devices

Related articles:

- [Auto-Provisioning Policy for EdgeMarc Devices](#)
- [Auto-Provision EdgeMarc Devices](#)

The Ribbon Application Management Platform (RAMP) lists the status of all the EdgeMarc devices that are provisioned with a policy. Use this procedure to view the provisioned status of each EdgeMarc device.

Prerequisites

- **Super User** [privileges](#) for **Insight Administration** under **Core Resources** are set
- **Devices, Provisioning Policy, and Resource Groups** [privileges](#) under **Device Management** are set

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Provisioning Status**. The "Provisioning Status" window displays.
3. In the option for **Last Known State**, select the status of devices you want to display in the table.
4. The table lists the devices based on the status you selected above.
5. To auto provision an EdgeMarc device, click **+Auto-Provisioning**. For more information, refer to [Auto-Provision EdgeMarc Devices](#).

Manage EdgeMarc Profiles

In this section:

- [Add EdgeMarc Profiles](#)
- [View and Edit EdgeMarc Profiles](#)

Related article:

- [Policy Parameters for EdgeMarc Devices](#)

Use the Ribbon Application Management Platform (RAMP) to add a new EdgeMarc profile, view details of existing EdgeMarc profiles, and edit an EdgeMarc profile. The **EdgeMarc Profiles** window lists the **Profile Name**, the associated **Resource Group**, the **Firmware Repository**, and the associated resource group **Policy**.

Prerequisites

- **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices, Resource Groups, EdgeMarc Profiles, Firmware Repository, and Provisioning Policy** [privileges](#) under **Device Management**.
- **Tenant Administration** [privileges](#) under **Authentication & Authorization**.

Add EdgeMarc Profiles

Use the following procedure to add a new EdgeMarc profile.

Start

1. Log on to the RAMP GUI.

2. Navigate to **Device Management > EdgeMarc Profiles**. The "EdgeMarc Profiles" window displays. Click **+ Add Profile**. The "Add Profile" window displays.
3. Select the **Tenant**.

Note

Only **Root** is supported as the Tenant.

4. Select the **Resource Group** to associate the EdgeMarc profile.
5. Select the **Firmware Repository** for the EdgeMarc profile.
6. To associate a resource group policy to an EdgeMarc profile, click **+Add Policy**. For more information on policy parameters, refer to [Policy Parameters for EdgeMarc Devices](#).
7. Click **Save**.

View and Edit EdgeMarc Profiles

You can create, update, and delete profiles for the resource groups to which your user group is provided access. For more information on user groups, refer to [Add User Groups](#).

Use the following procedure to view and edit EdgeMarc Profiles.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > EdgeMarc Profiles**. The "EdgeMarc Profiles" window displays. The EdgeMarc Profiles window displays the list of existing EdgeMarc profiles.
3. In the row for the EdgeMarc profile to edit, click the pencil icon under **Action** to open the EdgeMarc profile for editing.
4. Select the **Firmware Repository** for the EdgeMarc profile.
5. Click the policy name. The edit window for the associated policy displays. For more information on policy parameters, refer to [Policy Parameters for EdgeMarc Devices](#).
6. Click **Save**.

Policy Parameters for EdgeMarc Devices

The Ribbon Application Management Platform (RAMP) allows you to specify the policy parameters to apply on the EdgeMarc devices. The policy parameters listed in this section are applicable for both, resource group policy and auto-provisioning policy.

Prerequisites

- **Devices, Resource Groups, EdgeMarc Profiles, Firmware Repository, and Provisioning Policy privileges** under **Device Management**.
- **Tenant Administration privileges** under **Authentication & Authorization**.

Parameters to Create/Update a Policy

Parameter	Length/Range	Description
Policy Details		
Name	3-32 characters.	Provide a name for the policy. (Only alphabets, numbers, dashes, and underscores are allowed)
Description	0-255 characters.	Provide a description of the policy.
Tenant	N/A	Select the tenant. Note Only Root is supported as the Tenant.
Resource Group	N/A	Select the resource group.
Firmware Setting		
Note Firmware Versions are available only when you select a Resource Group.		
Upgrade Rule	N/A	Select a rule to upgrade the firmware. After you select the rule, select the Firmware Version . • Ignore • not less than: select a firmware version which is not lower than the options listed in Firmware Version. • not greater than: select a firmware version which is not greater than the options listed in Firmware Version. • must be equal to: select a firmware version which is equal to the options listed in Firmware Version.
Firmware Version	N/A	Select the firmware version. The available options are dependent on the selected Resource Group .
Configuration Setting		

Parameter	Length/Range	Description
Apply Configuration	N/A	Select one of the following: • Use Existing Configuration: select this option to use the existing configuration. Select an existing configuration. • Upload Configuration: select this option to upload a new configuration. Click Choose File, navigate to the location of the configuration, and upload the configuration.
Note Any changes made to the following configuration parameters overwrites the previous settings. For the new changes to apply, you must save it as a new configuration file.		
Network Settings		
EdgeMarc network settings		
Note Select the Push checkbox to edit and update the following parameters. By default the checkbox is not selected.		
LAN IPv4 Address	Provide the IPv4 address.	Provide a valid IPv4 address.
Prefix	1-32.	Provide the prefix.
LAN IPv6 Address		Provide the IPv6 address.
Prefix	1-128	Select the prefix.

Parameter	Length/Range	Description
WAN Interface IPv4 settings		Select the type of IP address. The options are: • Static IP • DHCP If you select Static IP: Provide the following details. • WAN IP Address: Provide the WAN IP Address. • Prefix: Select a value from 1-32. • WAN Gateway: Provide the WAN gateway.
WAN Interface IPv6 settings	N/A	Select one of the following: • Disable: Disables the WAN interface IPv6 settings. • Static IP: Provide the WAN IPv6 address, prefix (1-128), and the WAN gateway. • DHCP
Manually set DNS	N/A	Provide the following details: • WAN DNS Primary • WAN DNS Secondary
Enable SNTP	N/A	Provide the Time Server. For example, time.nist.gov.
Enable DHCP Server	N/A	Provide the following: • IP Address Range: If you have a range of IP addresses, provide the first IP address and the last IP address. • DHCP Server - Option 42: Provide a valid IPv4 or IPv6 address. • DHCP Server - Option 66: Provide a valid IPv4 or IPv6 address.
Secondary WAN Interface IPv4 settings	N/A	Select one of the following: • Disable Secondary WAN. • Static IP: Provide the WAN IPv4 address, prefix (1-32), and the WAN gateway. • DHCP.

Parameter	Length/Range	Description
Secondary WAN Interface IPv6 settings	N/A	Select one of the following: • Disable Secondary WAN. • Static IP: Provide the WAN IPv6 address, prefix (1-128), and the WAN gateway. • DHCP.
Manually set DNS for Secondary WAN	N/A	Provide the following: • Secondary WAN - DNS Primary • Secondary WAN - DNS Secondary
Security Settings		
Security Page	N/A	Select any of the following: • Allow SSH access through firewall • Allow HTTP access through firewall • Allow HTTPS access through firewall • Allow SNMP access through firewall There is no default value.
Admin/Service Config Settings		
Settings related to Admin / Service Config	N/A	Select any of the following: • Enable SNMPv1: ◦ Set SNMPv1 Read - Only Community: <TBD> ◦ Set SNMPv1 Host: Provide a valid IPv4 or IPv6 address. • Enable Remote System Logging: Provide a valid IPv4 or IPv6 address. • Enable MOS Scoring: Set the MOS scoring. The valid range is 0-5. • Enable Analytics: Set the Analytics Timeout. the valid range is 2-1666666. • Enable System Monitor: Enable this option to monitor the system.
Trusted Host Settings	Trusted Hosts allows a user to define a list of hosts or networks that are allowed to access this system via management protocols.	

Parameter	Length/Range	Description
Enable Trusted Hosts		Add Trusted Hosts: Provide the following information. Set IP Addresses for Trusted Hosts: Provide a valid IPv4 or IPv6 address. Port: Provide a port number from 1-32.
VOIP settings		
SIP protocol settings		Provide or select the following information: • SIP Server Name: Provide a valid IPv4 or IPv6 address. • SIP Server Port: The valid range is: 0-32768. • SIP Server Transport: Select one of the following transport types: ◦ Pass Through ◦ UDP ◦ TCP ◦ TLS • Use Custom Domain: ◦ SIP Server Domain: Provide a valid IPv4 or IPv6 address. • Enable Multi-Homed Outbound Proxy Mode: • Client UDP Listening Ports: Provide a value between 0-32768. • Enable LAN device UA name pass-through • Enable Transparent Proxy mode
Survivability Settings		

Parameter	Length/Range	Description
Settings related to Survivability Page		Provide or select the following parameters: • Enable Keepalives • Error codes: Provide a valid error code. • Rate - Pacing behavior: Select one of the following ◦ Configured Value: provide the configured value. • Rate-Pacing interval: Provide the rate pacing interval. The valid range is 1-999999. The default value is 1800. ◦ None (Rate-Pacing is disabled). ◦ Soft-Switch/IP PBX Provided Value. • Enable SIP server Redundancy: • Enable Phone Expires Override: Provide a value. The valid range is 0-999999. The default value is 20. • Monitor SIP Messages.

Upgrade Firmware for EdgeMarc Devices

The Ribbon Application Management Platform (RAMP) allows you to upgrade the firmware for selected EdgeMarc devices.

Prerequisites

- **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices, Resource Groups,** and **Job Status** [privileges](#) under **Device Management**.
- Firmware repository is created and available. It needs to be mapped with resource group on EdgeMarc Profiles page (Device section).

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Devices**. The **Devices** window displays.
3. Select the EdgeMarc device to upgrade the firmware.
4. From the **Bulk Actions** menu, select **Upgrade Firmware**. The **Upgrade Firmware** window displays.
5. The **Included Devices** panel lists the configured EdgeMarc devices on RAMP.
6. The **Excluded Devices** panel lists the configured EdgeMarc devices on which the firmware cannot be upgraded.
7. Use the following table to update the parameters and click **Save**.

Parameters

Parameter	Description	Length/Range
Upgrade to	Select the firmware version to upgrade.	N/A
Frequency		
One Time Only		
Perform Now	The default value is One Time Only, Perform Now .	
Perform Later	Select this option perform a restore on the date and time specified: • Date • Time	• 1-30 or 1-31, depending upon the calendar month. • 00:00:00-23:59:59
Comments	Enter an optional comment for your reference.	0-1500 characters.
Notification	Enable this option to receive in-app notification about the status when the particular action is completed. Note This option is only available when the Notification Service is deployed on the RAMP.	

View Attached Devices for EdgeMarc

The Ribbon Application Management Platform (RAMP) allows you to view the attached devices for a selected EdgeMarc device.

Prerequisites

- **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.
- Run the health check report. For more information, refer to [Run Health Reports on EdgeMarc Devices](#).

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Devices**. The Devices window displays.
3. In the nodes list, click on the **Node Name** of an EdgeMarc device to view its details.
4. Click the **View Attached Devices** tab.

The **View Attached Devices** displays the list of devices attached devices for this device.

View Call Charts for EdgeMarc Devices

The Ribbon Application Management Platform (RAMP) allows you to view the call data chart for a selected EdgeMarc device.

Prerequisites

- Available **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- Available **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management** > **Devices**. The Devices window displays.
3. In the nodes list, click on the **Node Name** of an EdgeMarc device to view its details.
4. Click the **Charts** tab.

The **Charts** tab displays the following details for WAN1 and WAN2 for the last 24 hours:

- MAC addresses.
- IPv4 and IPv6 addresses.
- WAN Status for the last 24 hours:
 - Grey depicts that WAN was either unreachable or down.
 - Green depicts that the WAN is up and running.
- WAN traffic (kb/s).
- WAN traffic by Queue. Enable the check boxes to view the details. The check boxes are enabled by default.
- Total peak calls.

Generate or Change Passwords

In this section:

- [Generate Passwords for Cloud-Based SBC or SLB Devices](#)
- [Generate Passwords for PSX Devices](#)
- [Change Password for EdgeMarc Devices](#)

The Ribbon Application Management Platform (RAMP) allows you to generate passwords for SBC, SLB, and PSX devices. You are allowed to change the password for EdgeMarc devices.

Generate Passwords for Cloud-Based SBC or SLB Devices

Ribbon Application Management Platform (RAMP) provides an option to update the password it uses to access interfaces on cloud-based SBC or SLB devices. When you invoke this option RAMP generates a password for each of the connection interfaces NETCONF, SSH/SFTP and LI and sends a change password request to the SBC or SLB device with the generated password. If RAMP receives a successful response from the device it updates the passwords stored on RAMP for the respective connection interface. If it does not receive a successful response from the device, RAMP retains the previous password.

Prerequisite

- The device is up and running.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the **Nodes** list row for the SLB or SBC device, click the ellipses (...) menu under **Action** and select **Generate SBC Password**.
4. Click **Generate Password** to confirm that you want to change the password.

Generate Passwords for PSX Devices

Ribbon Application Management Platform (RAMP) provides an option to update the password for the accounts it uses to access interfaces on primary PSX devices. When you invoke this option, RAMP generates a password for the `ems_<ip>` user and the `calea` user accounts on the PSX. If RAMP receives a successful response from the device it updates the passwords stored on RAMP for the respective accounts. If it does not receive a successful response from the device, RAMP retains the previous password. This option is not applicable to replica PSX devices or PSX devices in a GR configuration.

Note

- For Pre 15.x PSX, the change password option is supported only on the PSX primary nodes. It is not supported on the PSX GR and replica.
- For PSX 15.x and above, the change password option is supported only on the provisioning primary. It is not supported on the PSX primary and replica.

Prerequisite

- The device is up and running.
- You must have Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the **Nodes** list row for the PSX device, click the ellipses (...) menu under **Action** and select **Generate PSX Password**. A **Change Password** window opens.
4. Enter the current password for the PSX admin user.
5. Click **Generate Password**.

Change Password for EdgeMarc Devices

The Ribbon Application Management Platform (RAMP) provides an option to update the password for the EdgeMarc devices from the **Bulk Actions** Menu.

Prerequisites

- Available Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- Available **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Select the node that you want to change the password for.
4. From the **Bulk Actions** menu, select **Change Password**. The **Change Password** window displays.
5. The **Included Devices** pane lists the configured EdgeMarc devices on RAMP.
6. Update the password details and click **Save**:

Parameters

Parameter	Description	Length/Range
Fill in any passwords you wish to change. Empty fields will be unchanged	Select the Set all as option if you want change the CLI root password.	4-8 alphanumeric characters. Note Password must include at least one numeric character, one lowercase character, one uppercase letter, and one special character.
	Select the Set all as option if you want change the GUI root password.	
	Select the Set all as option if you want change the GUI Read-Only password.	
Frequency	The password change frequency. The frequency is a combination of One Time Only and either Perform Now or Perform Later . • One Time Only: Enabled by default. • Perform Now: Set password immediately. • Perform Later: Select the date to change the password.	
Comments	Provide optional comments for the reason to change the password. This has no system impact.	
Notification	Enable this option to receive in-app status notifications when a particular action is completed. Note You can view this option only when Notification Service is deployed on the RAMP.	

Job Status

The Ribbon Application Management Platform (RAMP) **Job Status** page displays the status of a job. For example, the status of back up or the diagnostic snapshot of an EdgeMarc device, etc.

Prerequisites

Devices, Resource Groups, and Job Status privileges under **Device Management**.

View Job Status

Perform this procedure to view the **Type, Job Type, Status, Key, Date/Time, and Source** of a job.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Job Status**. The **Job Status** window displays.

Note

The **Ring Buffer** details are displayed on the Job Status page only if **Action** is enabled. For more information, refer to [Create Trigger Notification Rules for EdgeMarc Devices](#).

Manage Clusters

In this section:

- [View and Edit Cluster Properties](#)
- [Duplicate Clusters](#)
- [Delete Clusters](#)
- [View Cluster Information and Status](#)
- [View History of Clustered Nodes](#)
- [Edit Configuration of SBC and SLB Devices in a Cluster](#)

The Ribbon Application Management Platform (RAMP) Device Management services provide a range of software and network management functions for both hardware-based and virtualized Ribbon devices. On RAMP, managed devices include both individual nodes and clusters. A cluster is a group of devices that share the same configuration and work together to perform a common network function. RAMP supports clusters providing PSX, SBC, and the SLB services.

After they register, navigate to **DEVICE MANAGEMENT > Devices** to manage the devices.

By default the **Devices** window open with the **Nodes** tab in view. Click the **Clusters** tab to see a listing all of the clusters that are currently registered. RAMP manages a cluster as a single device component. Each list entry on the **Clusters** tab provides a summary of information for the cluster, including its general status. Click on the cluster name to drill down to more details on the selected cluster. The options under **Action** enable you to perform actions on the corresponding cluster. The options that are available depend on the type of cluster and its current status.

The topics in this section describe specific ways you can work with clusters on RAMP.

Prerequisites for Managing Registered Devices

You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

View and Edit Cluster Properties

If needed, Ribbon Application Management Platform (RAMP) allows you to edit a cluster's configuration to change the properties associated with the cluster.

Prerequisite

- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click on the **Clusters** tab.
4. In the row for the cluster, click the pencil icon under **Action** to open the cluster configuration for editing. Note that some parameters can no longer be changed.
5. Refer to the parameter table for the type of cluster you want to edit.
 - a. To edit an SBC SWe cluster, refer [Create SBC Clusters](#).
 - b. To edit an SLB cluster, refer [Create SLB Clusters](#).
 - c. To edit a PSX cluster, refer [Create PSX Clusters](#).
6. Click **Save** to save your changes.

Duplicate Clusters

You can duplicate a cluster when you want to copy the configuration of an existing cluster to a new cluster. When you duplicate a selected cluster, Ribbon Application Management Platform (RAMP) creates a new cluster with the same basic settings and active configuration.

For SBC and SLB clusters, the devices in the duplicate cluster inherit the active device configuration of the original SBC or SLB cluster. Any SBC or SLB device registering to the new cluster receives this configuration.

Prerequisites

- You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. Click the **Clusters** tab.
4. In the row for the cluster you want to duplicate, click the duplicate icon under **Action**. An edit cluster window displays showing the settings of the original cluster.
5. Select or enter the values for the new cluster, including a unique cluster name and cluster identifier. Refer to the appropriate parameter table for information on cluster parameters:
 - a. For a PSX cluster, refer to [Create PSX Clusters](#)
 - b. For an SLB cluster, refer to [Create SLB Clusters](#)
 - c. For an SBC SWe cluster, refer to [Create SBC Clusters](#).
6. Click **Save**.

Delete Clusters

You can free up Ribbon Application Management Platform (RAMP) memory by deleting clusters from RAMP when they are no longer needed. Deleting a cluster deletes the nodes within the cluster along with configurations and other information related to the cluster. Before deleting a cluster, devices within the cluster must be unregistered.

Prerequisites

- Ensure that the nodes in the cluster are in unregistered state.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click the **Clusters** tab.
4. In the row for the cluster you want to delete, click the delete icon under **Action**.
5. Confirm the deletion when prompted.

View Cluster Information and Status

The Ribbon Application Management Platform (RAMP) provides details on cluster status and configuration. The details view for a cluster appears as a series of tabs that open from the **Devices** window, after you select a cluster name. Note that some tabs are specific to SBC or SLB clusters and appear only for those types of clusters.

- The **Overview** tab provides general status for a cluster and summarizes the current cluster configuration settings.
- The **Configuration** tab (SBC and SLB only) provides information on the active device configuration along with an option to edit it, and a summary of configuration history along with options to review or revert back to a prior configuration. Refer to [Edit Configuration of SBC and SLB Devices in a Cluster](#) for more information.
- The **Nodes** tab provides a list of nodes associated with the cluster.
- The **Redundancy Groups** tab (SBC only) provides details on the nodes within an SBC redundancy group.
- The **Status History** tab provides a list of the node status changes for the nodes that are configured within the cluster. Refer to [View History of Clustered Nodes](#) for more information.

Use the following procedure to see detailed information for a cluster.

Prerequisite

- You must have Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. Click the **Clusters** tab.
4. In the row for the cluster, click on the **Cluster Name** to open the cluster's detail view.
By default, RAMP opens an **Overview** tab for the selected cluster.
5. Click other tabs as needed to view additional types of information and options for the cluster.

View History of Clustered Nodes

You can view the history of status changes for the nodes that are configured within a cluster. After instantiating a device that is joining a cluster, check the node history to track the progress of the device.

Prerequisites

- You must have Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT** > **Devices**. The **Devices** window displays.
3. Click the **Clusters** tab.
4. In the row for the cluster, click on the **Cluster Name** to open the cluster's detail view.
5. Click the **Status History** tab to view the list of status change events for the cluster. The following table describes the type of data in the list.

Attribute	Description
Node Name	Name of the node.
VNFC ID	Identifier of the node.
Role	The role of the node. The following are the different roles: • Active • Standby • Standalone • Unknown "Unknown" indicates that a user deleted the node from a cluster and that another instance is using the IP addresses belonging to the instance.
Old App Status	The previous state of the node. The following are the different states of a node: • Registered: The node has sent a registration request. • Online: The node is registered and notified RAMP that the node is up. • Offline: The node is registered. It was online, but is no currently reachable. • Unregistered: The node is preserved in the database but is no longer managed. • NA: The node was never registered.
New App Status	The current state of the node. The following are the different states of a node: • Registered: The node has sent a registration request. • Online: The node is registered and notified RAMP that the node is up. • Offline: The node is registered. It was online, but is no currently reachable. • Unregistered: The node is preserved in the database but is no longer managed.
Timestamp	The time when the status changed.

Attribute	Description
Status Details	A description of the status change.

Edit Configuration of SBC and SLB Devices in a Cluster

Individual SBC or SLB nodes that are deployed as part of a cluster share the same device (SBC or SLB application) configuration. Ribbon Application Management Platform (RAMP) stores the device configuration for SBC or SLB clusters and also maintains a history of any configuration changes. When you edit the device configuration for the cluster, the configuration changes are stored on RAMP and pushed out to the nodes within the cluster so that the configuration of the nodes stay in sync. Thus, when you edit the device configuration of a cluster, you update the configuration of all of its nodes.

Note

A [duplicated](#) SBC or SLB cluster inherits its current active configuration from the source cluster. If a new node registers with RAMP and joins an existing cluster, it inherits its configuration from the cluster.

Edit Configuration of Devices in an SBC or SLB Cluster

User the following procedure to edit the device configuration for an SBC or SLB cluster.

Prerequisites

- At least one device exists in an OAM or Direct Single cluster.
- You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.
- You must have **GUI** and **Configuration Management** [privileges](#) under **Core Resources**.

Start

- Log on to the RAMP GUI.
- Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
- Click the **Clusters** tab.
- Click on the **Cluster Name** of an SBC or SLB cluster to open the details view of the cluster.
- Click the **Configuration** tab. The **Active Configuration** section provides summary information on the current configuration and an option to edit the configuration if needed.
- Click **Edit Configuration** to edit the active configuration. The SBC Configuration Manager window opens.
- Make the required SBC configuration changes. Refer to the [EMA User Guide](#) for more information about SBC configuration.
- Click **Apply Saved Changes and Close**.

RAMP triggers the active OAM node or active Direct Single node to save and apply the changes. The configuration is uploaded to RAMP and becomes the new active configuration. When the activation is complete, RAMP updates the **Configuration Activated** time adds another entry to the cluster's **Configuration History**. If the configuration fails to save to RAMP, replication still occurs, and the OAM/ Direct Single node retries saving the configuration

Work with Configuration History

Options in the **Configuration History** section on the **Configuration** tab enable you to work with prior versions of the cluster's configuration. For each version, you can view the associated changes, download the version or restore the cluster's configuration to that version.

Start

- Log on to the RAMP GUI.
- Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.

3. Click the **Clusters** tab.
4. Click on the **Cluster Name** of an SBC or SLB cluster to open the details view of the cluster.
5. Click the **Configuration** tab. The **Configuration History** section lists prior configurations stored for the cluster as **Revisions**, with the most recent revision at the top.
6. Under **Action**:
 - a. To **View Changes** made in a particular revision, click the lens icon. The **View Transaction Log** window lists the operations performed in the selected revision.
 - b. To **Restore** a configuration to a selected revision, click the circular arrow icon and confirm the configuration change when prompted.

Note

When you restore a configuration, the cluster nodes reboot which results in a temporary loss of service.

- c. To **Download** a configuration, click the download icon and confirm the download when prompted. The configuration file `<file name>.tar.gz` is downloaded to your local machine.
- d. To **Delete** a configuration, click the delete icon and confirm the deletion when prompted.

Launching Device GUIs from RAMP

Additional Topics:

- [Launch C20 GUI](#)
- [Launch DELL GUI](#)
- [Launch DSC GUI](#)
- [Launch DSI GUI](#)
 - [DSI Cluster](#)
 - [DSI Navigator](#)
 - [Trap Destinations](#)
- [Launch Edge 8000 GUI](#)
- [Launch EdgeMarc GUI](#)
- [Launch G5 GUI](#)
- [Launch G6MM GUI](#)
- [Launch GMS GUI](#)
- [Launch GSX GUI](#)
 - [Scheduling Report Data Collection](#)
 - [Creating Reports Using GSX Navigator](#)
 - [Event Log](#)
 - [Verifying the Database Status](#)
 - [Configuring GSX Call Trace Filters](#)
- [Launch IDH GUI](#)
- [Launch L2MGR GUI](#)
- [Launch PSX GUI](#)
 - [PSX GUI launch using OpenJDK](#)
- [Launch SBC Core and SLB GUIs](#)
 - [Mapping Between RAMP and SBC User Privileges](#)
- [Launch SBC Edge GUI](#)
- [Launch SGX GUI](#)
- [Launch STI GUI](#)

Ribbon Application Management Platform (RAMP) is the management client for registered devices that provide a Graphical User Interface (GUI) for configuration or management. You can launch the GUI for a device from RAMP without logging into each device individually.

The topics in this section describe how to launch the GUIs for different types of devices

Launch C20 GUI

Launch the C20 Call Session Controller (C20) GUI from Ribbon Application Management Platform (RAMP) to configure C20 devices.

Prerequisites

- The C20 device is registered on RAMP.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list row for the C20 device you want to configure, click on the ellipses (...) menu and select **Configure**. RAMP launches the Application Launching Point.
4. Select the application you want to access.
5. Log into the GUI using your login credentials.

For more information on configuring C20 devices, refer to [C20 Call Session Controller Documentation](#).

Launch DELL GUI

Launch the DELL GUI from Ribbon Application Management Platform (RAMP) to configure DELL devices.

Prerequisites

- The DELL device is registered on RAMP.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list, in the row for the DELL device you want to configure, click on the ellipses (...) menu and select **Configure**. The DELL Cockpit GUI opens.

4. Log into the GUI using your login credentials.

For more information on configuring DELL devices, refer to [Dell Server Deployment Guide](#).

Launch DSC GUI

Launch the DSC Manager GUI from Ribbon Application Management Platform (RAMP) to work with Diameter Signal Controller (DSC) devices.

Note

RAMP does not support Single Sign-on (SSO) for the device on-board management interface.

Prerequisites

- The DSC device is registered on RAMP.
- The DSC device is up and running.
- You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

To launch DSC Manager:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window opens.
3. In the nodes list, in the row for the DSC device you want to configure, click on the ellipses (...) menu and select **Configure**. The DSC login window displays.
4. Log into DSC to open the DSC Manager. For more information on working with DSC, refer to [Diameter Signaling Controller 23.0.x Documentation](#).

Launch DSI GUI

Related articles:

- [DSI Cluster](#)
- [DSI Navigator](#)
- [Trap Destinations](#)

Launch the DSI Manager GUI from Ribbon Application Management Platform (RAMP) to work with DSI devices. The DSI Manager contains two tabs:

- **Navigator**
Displays a node tree of DSI objects and allows basic management operations on any registered DSI. Allows you to perform a wide range of management and maintenance tasks on registered nodes.
- **Trap Destinations**
Allows you to define trap destinations for selected, registered nodes. You must have DSI Super User privileges in order to access the DSI Manager.

Prerequisites

- The DSI device is registered on RAMP.
- The DSI device is up and running.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

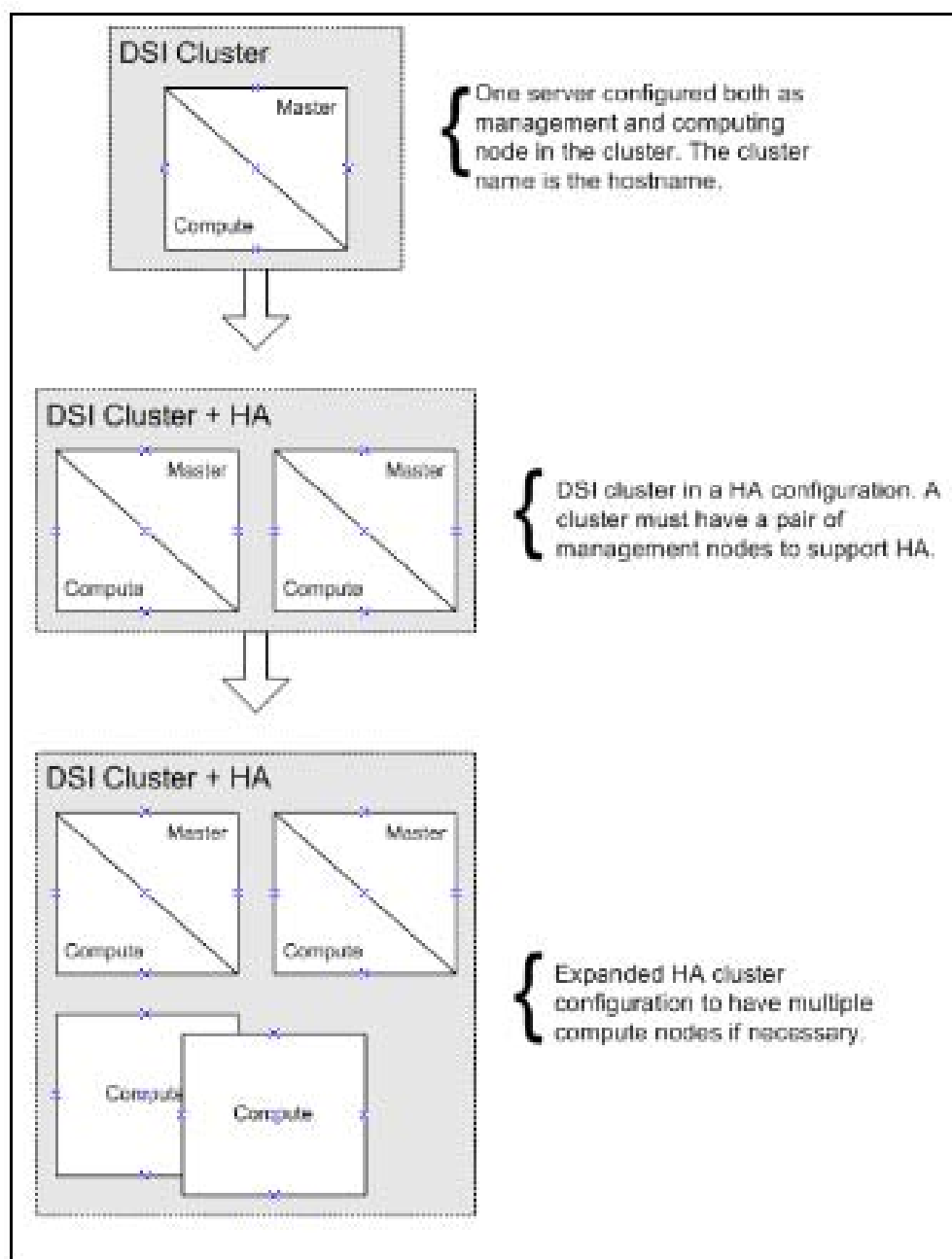
1. Log on to the RAMP GUI.
2. Navigate to **Device Management** > **Devices**. The **Devices** window displays.
3. In the nodes list, in the row for the registered DSI device you want to configure, click on the ellipses (...) menu and select **Configure**. The DSI Manager window opens. Refer to the topics under [DSI Cluster](#) and [DSI Navigator](#) for more information on using DSI Manager.

DSI Cluster

Related articles:

- [Sun Cluster Manager](#)

A DSI cluster is a group of servers, which presents itself as a single logical system to clients outside the cluster. There are two types of nodes in a cluster: an Mnode, which is a management (or master) node and a Cnode (compute) node. Mnodes also function as compute nodes and have the responsibility for managing the cluster, including collecting and distributing billing data to the Cnodes. Also, unlike Cnodes, Mnodes are connected directly to the shared storage device. Cnodes have the responsibility for providing data services on the billing data received from the Mnode. A cluster can contain a maximum of three Mnodes (in an HA configuration) and many Cnodes, to a maximum of 16 nodes total.



Sun Cluster Manager

Related articles:

- [Enabling Web Server on a DSI Device](#)
- [Accessing DSI Cluster Details](#)

The Sun Cluster Manager is a GUI that enables you to perform the following:

- Display graphically the cluster information
- Monitor configuration changes
- Check the status of the cluster components
- Perform administrative tasks for Sun Cluster components such as Adapters, Cables, Data services, Global services, Interconnects, Junctions, Nodes, Quorum devices, Resource groups, and Resources.

The Launch Cluster Page icon is available only after selecting the DSI device. After the icon appears, perform the following procedures:

- ✓ Enabling webserver on the selected DSI device
- ✓ Accessing DSI cluster details

Enabling Web Server on a DSI Device

To enable the web server, perform the following procedure:

1. Log into the DSI Node as `root` user.
2. Enter the following commands in the bash shell:

```
svcprom /system/webconsole:console | grep tcp_listen options/tcp_listen boolean  
false  
netstat -a | grep 6789  
/usr/sbin/smcwebserver status
```

3. The following message appears:

```
Sun Java(TM) Web Console is running
```

4. Enter the following command:

```
svccfg
```

5. The following message appears:

```
svc:> select system/webconsole  
svc:/system/webconsole> setprop options/tcp_listen=true  
svc:/system/webconsole> quit
```

6. Enter the following command:

```
/usr/sbin/smcwebserver restart
```

7. The following message appears:

```
Restarting Sun Java(TM) Web Console Version 3.1 ...  
The console is running
```

After enabling the web server, click the Launch Cluster page icon to access the Java Web Console page.

Accessing DSI Cluster Details

To access the DSI cluster details, perform the following procedure:

1. Enter the user name and password in the User Name and Password fields.
2. Click **Login**.
The Java Web Console page appears.
3. Click the Sun Cluster Manager link.
The DSI cluster details appear.

DSI Navigator

Related articles:

- [Cluster Manager](#)
- [Adaptor](#)
- [Adaptor DB Info](#)
- [ADBI \(Ancillary DB Interface\)](#)
- [CAM Management](#)
- [Closure Spec](#)
- [Code Set](#)
- [Connection Alarm Timer](#)
- [Correlation Rules](#)
- [Data Route](#)
- [Data Server](#)
- [DSI Configuration](#)
- [DSI Health Monitor](#)
- [DSI Health Monitor Log](#)
- [DSI Transporter Client](#)
- [File Services](#)
- [File Spec](#)
- [File Template](#)
- [FTP Client](#)
- [FTP Daemon](#)
- [IMDS](#)
- [Input Connector](#)
- [Load Balancer Configuration](#)
- [Maintainer](#)
- [MATS BE Server](#)
- [Operating Modes](#)
- [Output Connector](#)
- [Package](#)
- [Ports](#)
- [Route Definition](#)
- [RSN Sequence](#)
- [RSN Spec](#)
- [Stream Configuration](#)
- [Stream Processor](#)
- [DataStream Integrator Object](#)
- [Alarm Manager](#)

- [Host Resources](#)
- [Log Manager](#)
- [NFS Configuration](#)

The DSI Navigator provides a navigation tree, allowing you to perform management operations on any DSI Cluster or Cluster member (Mnode or Cnode). Through the DSI Navigator you can access the following functional categories:

The DSI Navigator objects are classified in two types:

- Cluster Level Objects
- DSI Level Objects

The following table list the DSI Navigator Objects.

DSI Navigator Objects

Cluster Level Objects	
Cluster Manager	Adaptor
Adaptor DB Info	ADBI (Ancillary DB Interface)
CAM Management	Closure Spec
Code Set	Connection Alarm Timer
Correlation Rules	Data Route
Data Server	DSI Configuration
DSI Health Monitor	DSI Health Monitor Log
DSI Transporter Client	File Services
File Spec	File Template
FTP Client	FTP Daemon
IMDS	Input Connector
Load Balancer Configuration	Maintainer
MATS BE Server	Operating Modes
Output Connector	Package
Ports	Route Definition
RSN Sequence	RSN Spec
Stream Configuration	Stream Processor
DSI Level Objects:	
DataStream Integrator	Alarm Manager
Host Resources	Log Manager

NFS Configuration	

For additional information concerning the operation and administration of the Ribbon DSI, refer to the DSI documentation set.

You begin to use the DSI Navigator by selecting a Cluster or Device from the Device Selection list. The list displays Cluster names in white lettering on a green background; Mnodes are in green lettering preceded by a dash; Cnodes are in black lettering preceded by a dash; Standalone nodes are in black lettering. According to the Cluster/Device you select from the Device List, the object tree displayed in the left pane (see the table given below) changes. Each category shown in the DSI Navigator tree represents a function or functional area of the DSI. To access commands pertaining to a specific area, simply click on the category or subcategory and the command drop-down list changes to a command list pertaining to that category. The sections that follow discuss the categories and commands available for each.

Note

The system displays nodes that are not currently associated with a cluster as members of an orphan cluster. The orphan cluster and its members display in the same manner as regular clusters.

Selected Device Tree Elements

Category	Cluster Level	Node Level
Cluster Manager	X	
Data Stream Integrator		X
Data Server	X	
(Data Server) Data Manager	X	
(Data Server) AMA	X	
Alarm Manager		X
DSI Configuration	X	
DSI Health Monitor	X	
DSI Health Monitor Log	X	
FTP Client	X	
Host Resources		X
Log Manager		X
Maintainer	X	
(Maintainer) House Keeping	X	
MATS BE Server	X	
FTP Daemon	X	
Route Definition	X	
Output Connector	X	
Input Connector	X	
Load Balancer Configuration	X	

Category	Cluster Level	Node Level
DataRoute	X	
Package	X	
(Package) Adaptor	X	
Adaptor	X	
Adaptor DB Info	X	
Ports	X	
Code Set	X	
(Code Set) NV Pair	X	
(ADBI) SRS	X	
Operating Modes	X	
File Services	X	
File Services Source	X	
DSI Transporter Client	X	
DSI Transporter Client Source	X	
DSI Transporter Client Destination	X	
Stream Processor	X	
Correlation Rules	X	
Connection Alarm Timers	X	

Cluster Manager

The Cluster Manager command menu allows you to remove a node from the cluster, check the status of the cluster and start/stop/reload/update all or individual cluster nodes. The table below provides information concerning the available commands and their use.

DSI Cluster Manager Commands

Command	Definition
Add Node	Adds the named node to the cluster.
Remove Node	Removes the designated node from the cluster. If there is only one Mnode in the Cluster, you cannot remove it.
Show Cluster Status Show All Node Status Show Private Network Status Show Public Network Status Show Resource Group Status Show Shared Disk Status	The Show commands display the status of the designated object. The Show Cluster Status command include the information displayed in all of the other show commands.
Stop All Nodes	Stops DSI services (TP, Maintainer, etc.) on all nodes in the cluster.
Reload All Nodes	Reloads the transaction processor and the maintainer by stopping and then restarting them). Use this command to reload the ConnectorDefinition so that the new settings take effect, or to register new adaptors with DataStream Integrator.
Start All Nodes	Starts DSI services (TP, Maintainer, etc.) on local or all nodes in the cluster.
Stop Node	Performs the same function as the Stop All Nodes command, except the action impacts only the node specified.
Reload Node	Performs the same function as the Reload All Nodes command, except the action impacts only the node specified.
Start Node	Performs the same function as the Start All Nodes command, except the action impacts only the node specified.
Reload File Services	Implements modified global or individual source configurations while FileServices is running.

If the cluster contains only Level 0 and Level 1 DSIs, the only commands available from the Cluster Manager object are Start Node, Stop Node, Reload Node, and Reload File Services.

Adaptor

The Adaptor category provides information concerning the version numbers and names of the various AMA and CAM adaptors installed on your DSI by executing the **Show** command. You can also remove an Adaptor by selecting it from the list (checking the select check box) and executing the Remove command from the Command List.

Adaptor DB Info

You can use the Adaptor DB Info object to define the database users parameters used by the correlation adaptor. To change any parameters, select the adaptor from the list by checking the Select check box and executing a **Show** command.

Adaptor DB Info Field Definitions

Field	Definition
Adaptor Name (read only)	The name of the selected adaptor.
User Name	Defines the database user name.
Password	Defines the database user password.
Database Instance	Defines the database instance.
Retry Attempts	Defines the number of database connection retry attempts.
Delay in Seconds	Defines the delay (in seconds) between attempts to connect to the database.

After changing any of the parameter values, click the **Update** button to save you changes.

ADBI (Ancillary DB Interface)

The ADBI category contains SRS (Subscriber Reporting Server) child object used to configure parameters for the operation of the SRS. The ADBI SRS supports GSX CDRs. Refer to the table below for definitions of the parameters.

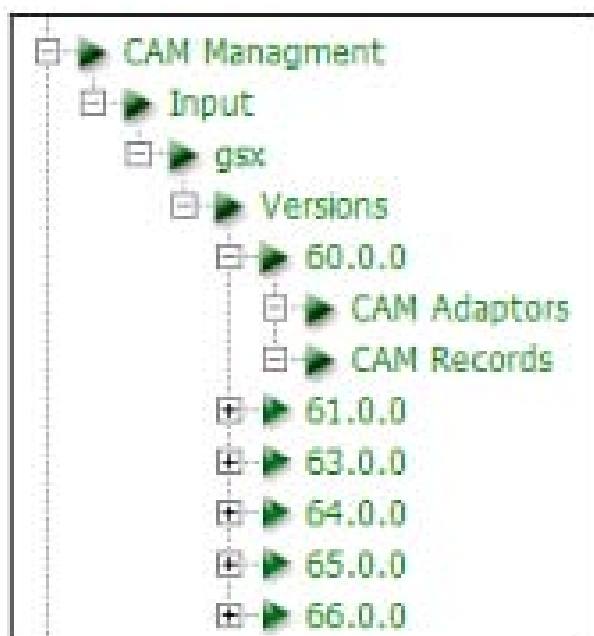
SRS Update Field Definitions

Field	Definition
User Name	The database user name for the SRS Database
Password	The user password for the SRS Database
SRS Database ID	The database ID for the SRS Database
Local Log File	The location of log file to record SRS Database load errors
Remote Script Directory	The remote script directory
Remote Output Directory	The remote output directory
Remote Processing Directory	The staging location for CSV files during SRS Database loading
Local Control File	The location of control file which defines CSV data structure to load
Local Working Directory	The staging location for CSV files prior to SRS Database loading
Local Sleep Time	Defines the scanning period to inspect for newly staged CSV files.
Local Timeout	Timeout period in seconds.

After making any changes click the **Update** button to save your changes.

CAM Management

The CAM Management section of the DSI Cluster Manager tree allows you to select the particular fields from the various types of CDR record types that the Stream Server requests from the Stream Client. The following figure provides an example of the tree structure and the table provides information concerning the available commands.



CAM Management Commands

Command	Tree Object(s)	Command Definition
Show	Input Input Instance (for example, gsx in the figure above) Version Instance (for example, 60.0.0 in the figure above) CAM Adaptors CAM Records	Shows either a list of the child objects, or the current configuration for the selected record type and input device depending upon the selected object
Show Consolidated	Version Instance (for example, 60.0.0 in the figure above) CAM Adaptors	Lists a consolidated view of the mappings of field ID to field name for BCAM production for each type of record.
Show Mappings	Version Instance (for example, 60.0.0 in the figure above)	Lists the mappings of field ID to field name for BCAM production.
Show Missing	CAM Records	Lists the field IDs not included in the current configuration for the particular version of input device
Show Mandatory	CAM Records	Lists the mandatory fields for valid record(s) for BCAM production.
Show Valid	CAM Records	Lists the fields for valid record(s) for BCAM production.

Command	Tree Object(s)	Command Definition
Commit Changes	CAM Records	Implements the changes

Closure Spec

The Closure Spec object allows you to configure a number of parameters that consolidate AMA Output records based on recordcount, filesize, or timeinterval criterion. To establish a new Closure Spec object, select Closure Spec from the object tree and select **Create** from the Command list. See the table below for definitions of the parameters. To edit an existing object, select it from the list and select the **Show** command.

Closure Spec Field Definitions

Field	Definition
Name	The name assigned to this output file closure specification.
Record Count	Defines the number of records per CDR output file. The valid range is between 0 and 4294967295, where an entry of 0 disables this parameter. There is no default value.
The system considers both the Record Count and File Size parameters with whichever value satisfied first taking precedence.	
File Size	Defines the maximum size of the CDR output file. The range of allowed values is between 0, which disables this parameter, and one of the following: • 1073741824, if you do not define the units, • 1048576, if you define kilobytes (K) as the units, or • 1024, if you define megabytes (M) as the units.
Sequence Reset	Indicates whether or not the system resets sequence number after each closure. If checked, the system resets the sequence number; if unchecked (default) the system does not reset the sequence number.

Field	Definition
Time Close	Specifies the time at which to start a new file in the output file consolidation. The entry must conform to the following syntax: minutes (0 to 59), hour of day (0 to 23), day of month (1 to 31), month of year (1 to 12), and day of week (0 to 6, where 0 is Sunday). Separate each field entry with a space and multiple entries in a field by a comma. You may specify a range of values in a field by using a dash. An asterisk in any field signifies all valid values. For example, an entry of 15 3 * * * would result in the system force closing the files at 3:15 AM every day of every month. or 30 0,12 * * 15 would result in the system force closing the files at 12:30 AM and 12:30 PM, Monday through Friday. An entry of “—” (without quotes) disables the argument.
Exposure	Specifies the usage of this output file closure specification as either: • local — specifies the output file closure specification is associated with only one connector object. • global — specifies the output file closure specification is associated with any number of connector objects

After making any changes click either the **Submit** or **Update** button to save the object.

Code Set

DSI provides a facility known as a CodeSet Table. Each entry in a CodeSet Table is composed of a pair of discrete values that are related such that, if the key discrete value is observed in a data field to be translated by DSI, the translation applied is to replace the key lookup discrete value in the CodeSet with its associated discrete value. A simple example is substitution of a postal state abbreviation for the complete state name (for example, “VA” replaced with “Virginia”). Another example would be a CodeSet formed of network device names as they are known on either side of a network.

CodeSet Tables define one or more pairs of CodeSets. CodeSets are available only through CodeSet Tables and CodeSet Tables can only be used by adaptors. Furthermore, an adaptor must have been constructed with specific knowledge of a particular named CodeSet table and have that CodeSet table included within the adaptor structure before the CodeSet Table can be utilized. For any adaptor having this capability, the CodeSet Table, having already been defined, can be maintained through the CLI. Entries can be added, changed, or deleted.

Changes can be submitted to a draft workspace CodeSet Table and batched into a single transaction before taking effect. The batch transaction takes effect only when expressly committed by the user. The user can control how many changes to batch together, visually inspect the batched changes prior to committing the changes, compare the batched changes against the current master CodeSet Table, and either commit the currently batched changes or roll them back to the master CodeSet Table. When the batched changes are committed, they immediately take effect. That is, the next job initiated for DSI processing leverages the updated master CodeSet Table specifications.

Refer to the [Administering and Maintaining DSI](#) documentation for information concerning the creation of Code Sets.

Only an adaptor constructed with specific knowledge of a particular named CodeSet table can utilize the Code Set Pairs within the table.

Connection Alarm Timer

The Connection Alarm Timer object, visible when viewing an MNode, allows you to configure Alarm Timer settings for **TCP** and/or **File** connection types.

Selecting either the TCP or File tree object, the **Show** command displaying the current configuration of the selected Connection Alarm Timer. To change the configuration of the timer, enter new values in the fields and click the **Update** button. The field definitions are given in the Table below.

Connection Alarm Timer Field Definitions

Field	Definition
Connection Type (read only)	Either TCP or File based upon the tree object selection.
Input Idle Timer	If there is no input activity for the specified time, the system generates an alarm indicating the lack of input activity. The valid range is between 0 and 168 hours with a default setting of 1. An entry of 0 disables the timer.
Output Idle Timer	If there is no output activity for the specified time, the system generates an alarm indicating the lack of output activity. The valid range is between 0 and 168 hours with a default setting of 1. An entry of 0 disables the timer.
Enable Input Idle Timer	Enables (checked) or disables (unchecked) the Input Idle Timer.
Enable Output Idle Timer	Enables (checked) or disables (unchecked) the Output Idle Timer

Correlation Rules

The Correlation Rules object allows you to associate or disassociate Correlation Rules with one or more Sensor IDs. You can view the current association(s) by selecting a rule from the list and executing the **Show** command. There are two additional commands available after selecting this object: **Add Sensor ID** and **Remove Sensor ID**. In either case the only editable field is the ID field where you enter one or more IDs separated by commas and then click the **Submit** button.

Data Route

The Data Route category lists defined communication routes. The actual definitions reside in the DataRoute file. From this section you can create, edit, or delete Data Routes.

To create a new Data Route, select Create from the command list and complete the fields using the definitions in the table as a guide.

Data Route Configuration

DSI Manager

Navigator | **Trap Destinations**

Devices: emsdsi Cluster ▾ Data Route Commands: Create ▾ Select

DSI

Cluster Manager

Adaptor

Adaptor DB Info

ADBI

CAM Managment

Closure Spec

Code Sets

Connection Alarm Tin

Correlation Rules

Data Route

Data Server

DSI Configuration

DSI Health Monitor

DSI Health Monitor Lo

DSI Transporter Clie

File Services

File Spec

File Template

Ftp Client

Ftp Daemon

IMDS

Input Connector

Load Balancer Config

Maintainer

MATS BE Server

Operating Modes

Output Connector

Parkage

Name *:

IP Address *:

Handler *: 3RD ▾

Connection Type *: Push ▾

Directory *: /export/home/SonusNFS ▾

Port (1-65535) *:

Archive Files ☐

Archive Directory:

User ID *:

Password *:

Working Directory *:

Process Type *: Client ▾

Active ☐

Ftp Frequency (1-86400):

PASV Port (10000-65535):

PASV Port Range (1-55535):

Audit ☐

* Required

Submit Reset

Create Data Route Field Definitions

Field	Definition
Name	A unique name designating the Data Route instance. The maximum field length is 32 characters.
IP Address	Provides the address of the remote system with which the DSI establishes a data connection.
Handler	Defines the handler type: DSI for data routes between DSI Transporter Client and DSI. 3RD for data routes including third-party servers.
Connection Type	Defines the method of connection as either Push or Pull .
Directory	Defines the directory on the remote system to place the file (used for client process types)
Port	The port to connect to for a client process or the port to accept a connection from for a server process. The allowed range is between 1 and 65535.
Archive Files	If checked, the DSI creates an archive file.
Archive Directory	Defines the directory used to store archive files.
User ID	The user name used to connect to a remote system, or to accept from a remote system.
Password	The password associated with the User ID.
Working Directory	Defines the temporary directory used to maintain the data during processing.
Process Type	Defines the process type as either Client or Server .
Active	Enables client (1) or disables client (0) by including or removing from inittab file. It is used only for Transporter processes on DSI server only. By default, the value is set to 0.
Ftp frequency	Defines the time required for the transporter client to perform FTP to Transporter Server. This field is valid for CommCIntConfig. The default value for this parameter is 60.

Field	Definition
PASV Port	The IP port for passive FTP operation. This field is valid only for commSvr entry in CommConfig and CommSvrConfig files.
PASV Port range	The number of IP ports starting from pasv_port allowed for passive FTP operation. This field is valid only for commSvr entry in CommConfig and CommSvrConfig files.
Audit	Used to enable/disable auditing.

The other operations which can be performed on the data routes include:

- **associateClient** — Acquires the list of destination(s) and associates the destination(s) to DSI remote client. Supports association of only one destination by default. Broadcast license is required to associate more than one destinations.
- **listAssociations** — Lists the destinations associated to the remote client.
- **disassociateClient** — Disassociates destination(s) from DSI remote client.

Data Server

The Data Server is the DSI component that receives Call Account Message (CAM) files from a generating system (a system that produces CAM data), processes the records converting CAM files to standard AMA data file format, and transfers the files to a Data Manager.

When you select the Data Server object from the tree, the **Show** command executes automatically. To update the configuration of the Data Server, click on the **Data Server** category in the object tree to display the Data Server fields in the right pane. Edit the fields using the definitions shown in the following table as a guide and click the **Update** button.

Data Server Field Definitions

Field	Definition
Source Component Type	Specifies the source component type. The range is from 1 to 15. The default setting is 2.
Source Component ID	Specifies the source component ID. The range is from 0 to 4095.
Recording Office ID	Specifies the data server's recording office ID. The range is from 0 to 999999.
Recording Office Type	Specifies the data server recording office (sensor) type. The range is from 0 to 999. The default value is 199.
Record Source Type	If checked, the source component type and source component ID are recorded in each AMA file header.
Push Files	If checked the system pushes AMA files through FTP Push.
Field Suppression	Specifies the fields suppressed in the AMA output record. Valid values are: • 0 no suppression • 2 two fields suppressed: Recording Office ID and Type • 4 four fields suppressed: Recording Office ID and its Type, and Sensor ID and its Type

Additional sections:

[AMA](#)

[Data Manager](#)

AMA

You can use the AMA subcategory to configure various parameters used in the creation and transmission of AMA files. To set the parameters, select AMA in the Navigator tree and enter the necessary information in the fields based upon the definitions supplied in the following table.

If you select an AMA file under the Primary AMA navigator tree object, there are three additional commands available. The **Show** command displays the filename of the selected AMA file, the **Convert** command converts and displays the file contents, and the **Mark for Relocation** command designates the selected Primary AMA file for relocation to the archive directory (Secondary AMA).

Note

Use the Mark for Relocation option only after you confirm that either the primary AMA file is unnecessary or that the primary AMA file was already sent, but not demoted to secondary status.

Since AMA files located under the Secondary AMA navigator tree object are files relocated from the Primary AMA location, you can only run the **Show** command.

Note

On the DSI, the Primary AMA files are located in the /dsi/batch/AMAFiles directory. The Secondary AMA files are located in the /dsi/batch/AMAFiles/archive directory.

AMA Field Definitions

Field	Definition
Destination Component ID	Specifies the destination component ID that will be used for all data managers. The range is 0 to 4095.
Destination Component Type	Specifies the destination component type that will be used for all data managers. The range is 1 to 15. The default setting is 3.
Enable Tracer Records	If checked, the DataStream Integrator generates primary and hourly tracer records.
Enable Standard File Extension	When checked the DSI uses standard AMA filenames; when unchecked the DSI uses the specified Alternate Filename.
Alternate File Extension	Specifies the alternate file name, if you choose not to use the standard AMA naming convention. For example, typing Stream7 will result in an output file name of Stream7.nnnn where nnnn is the sequence number.
Max Records per File	Specifies the maximum number of records for a resulting AMA output file. A setting of 0 means an unlimited number of records.
Max Bytes per File	Specifies the maximum number of bytes for a resulting AMA output file. A setting of 0 means an unlimited size.
Force Close	Specifies the times (times, days, and dates) for the system to run a cron job automatically closing the input files. The entry must conform to the following syntax: minutes (0 to 59), hour of day (0 to 23), day of month (1 to 31), month of year (1 to 12), and day of week (0 to 6, where 0 is Sunday). Separate each field entry with a space and multiple entries in a field by a comma. You may specify a range of values in a field by using a dash. An asterisk in any field signifies all valid values. For example, an entry of 15 3 * * * would result in the system force closing the files at 3:15 AM every day of every month. or 30 0,12 * * 15 would result in the system force closing the files at 12:30 AM and 12:30 PM, Monday through Friday.
Enable Ascii Generation	If checked, instructs the DataStream Integrator to generate AMA files in ASCII format.
Max Size per Recovery File	Specifies the maximum size of the recovery files. The default size is 10MB but the file can be from 10KB to 50MB.

Data Manager

The Data Manager category of the DSI Manager object tree, located under the Data Server category, lists all configured data managers on the DSI. You can have a maximum of 4 adapters configured (numbered 1 through 4).

To create a new adaptor instance, select Create from the Data Manager command list and complete the fields based upon the definitions provided in the table below.

There are two commands available for the adapters listed under the Data Manager, **Show** and **Remove**. The Show command displays the current configuration of the selected Data Manager instance. To change the configuration of the adapter, enter new values in the field and click the **Update** button. To delete an adapter, select the delete command and click the **Select** button.

Important

There is no confirmation message associated with the delete command. Verify that you selected the adapter you wish to delete prior to executing the command.

Data Manager Field Definitions

Field	Field Location	Definition
Primary	Create, Show	If checked, sets this DM to be the primary DM. You may have only one primary DM at any time. If you do not manually set one DM as primary, the system designates the first DM as primary.
Host	Create, Show	Specifies the host name of the DM. This entry must be between 3 and 14 characters in length.
Push IP Address	Create, Show	Specifies the IP address of the data manager.
Push Port	Create, Show	Specifies the listening port used by the data manager to receive data.
Push Login	Create, Show	Specifies the logon name used by the data server to connect to the data manager. The logon name must be between 3 and 9 characters in length. The system uses this entry in combination with the Push Password entry.
Push Password	Create, Show	Specifies the logon password used by the data server to connect to the data manager. The system uses this entry in combination with the Push Login entry.
Enable Passive FTP	Create, Show	Specifies if the data manager allows a passive FTP connection from the data server. The default setting is checked, allowing passive FTP connection.
Pull Login	Create, Show	Specifies the logon name used by the data manager to connect to the data server. The logon name must be between 3 and 9 characters in length. The system uses this entry in combination with the Pull Password entry.
Pull Password	Create, Show	Specifies the logon password used by the data manager to connect to the data server. The password must be between 6 and 8 characters long, with at least 2 alphabetic characters and at least one numeral or special character. The system uses this entry in combination with Pull Login entry

Field	Field Location	Definition
Absolute Path	Create, Show	Specifies the directory where the Data Server pushes ftp files.
Use Absolute Path	Create, Show	Specifies if the Data Server uses the absolute path when pushing ftp files. If checked, you must specify an absolute path.
Rename	Create, Show	Specifies if the Data Manager expects DataStream Integrator to rename a pushed file.
Index	Create, Show	A unique index number designating the Adaptor instance. The entry must be between 1 and 4.

DSI Configuration

Additional articles:

- [Import Policy](#)

The DSI Configuration object has two child objects, Configuration and Import Policy, that allow you to export and import DSI configurations from one cluster to another. This feature eliminates the need to manually provision multiple nodes and avoids errors in provisioning discrepancies between the two cluster instances. While the number of nodes in the source and target cluster can differ, the following characteristics must match for each cluster:

- DSI license level
- DSI application version (except patch level)
- DSI application operating mode configuration
- Checksum of each export/import component

The Configuration object displays any exported configurations resident on the cluster. Before selecting a saved configuration, there is only a single command available, Export DSI Configuration. Executing this command opens a dialog box containing a single field for the **Name** of the saved file. After entering a name (32 character maximum and must begin with a letter) and clicking the **Submit** button to start the export process.

The export process saves the source DSI configuration into a single encrypted tar file with an accompanying checksum (.md5) file. These files are stored in the global/home/dsi/<dsi version>/export/rep directory with the name name.hostname.clustername.DSI version.date/timestamp where:

- name — the value you entered in the Name field.
- hostname — the hostname of the DSI server.
- clustername — the clustername of the cluster.
- DSI version — the software version running on the DSI, such as DSI_V07.01.00R000.
- date/timestamp — the date and time of the export in the form YYYY_MMDD_HH:MM:SS where the HH ranges from 0...23.

When the export completes, a report of files collected and their checksum values is written to the DSI log file and appear as child objects under the saved configuration object.

Note

To make an exported configuration available for importing on another cluster, you must move the tar file and .md5 file from the global/home/dsi/<dsi version>/export/rep directory on the source server to the same directory on the target server.

After selecting a saved configuration, the following additional commands become available:

- Show Configuration — Displays information concerning the selected configuration
- Compare Configuration — Compares the selected configuration to the current configuration

Note

On T5220 DSI, you need to disable the encryption algorithms on all the nodes before comparing the configurations.

Refer to **Commands in configmanager Subsystem**, [DataStream Integrator CLI](#) in DSI documentation for more information.

- Validate Configuration — Validates the selected configuration
- Delete Configuration — Deletes the saved configuration
- Import Configuration — Imports the selected configuration (also see Import Policy)

Also, under each saved configuration there are two child objects, DSI Application Configuration and DSI System Configuration. From each of these child objects you can access individual component configurations by checking the desired item in the list and executing the **Show** command.

Import Policy

The Import Policy allows you to configure the items imported when you execute an Import Configuration command. You select an item for importing by selecting the appropriate check box . After making any changes to the Import Policy, click the **Update** button to save the changes.

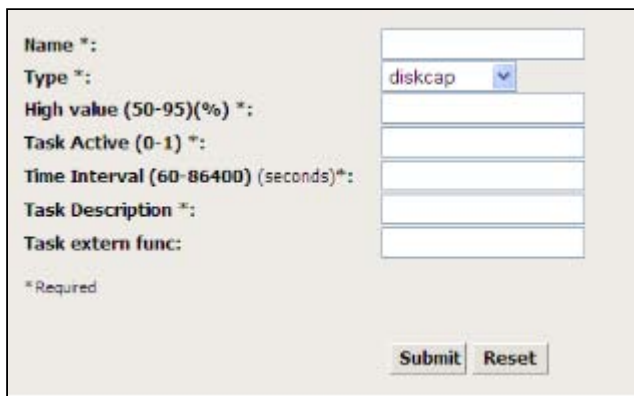
Profile :	☒
RSN SPEC DB :	☒
FSN SPEC DB :	☒
CLS SPEC DB :	☒
FTP Status DB :	☒
ADBI Configuration :	☒
DSDM Configuration :	☒
Stream Configuration :	☒
Comm Configuration :	☒
Comm Client Configuration :	☒
FS Configuration :	☒
FS Source Set :	☒
SAI Configuration :	☒
Connector Definition :	☒
Route Definition :	☒
House Keeping :	☒
Init Tab :	☒
Init Tab2 :	☒
Init Tab3 :	☒
TNS Names :	☒
Adaptor DSI Configuration :	☒
Adaptor DSI spec :	☒
DSI Alarm :	☒
Alarm Config :	☒
BCAMSelfRecord :	☒
CDR tracking :	☒
imdsConfig :	☒
MATS Files :	☒

DSI Health Monitor

Additional articles:

- [DSI Health Monitor Tasks](#)

The DSI Health Monitor object allows you to create tasks that periodically performs health checks on predefined operational configuration, application state, system resources, connection interfaces with peer hosts, or other environmental factors.



The screenshot shows a configuration form for a DSI Health Monitor task. The form has the following fields and controls:

- Name *:** A text input field.
- Type *:** A dropdown menu with "diskcap" selected.
- High value (50-95)(%) *:** A text input field.
- Task Active (0-1) *:** A text input field.
- Time Interval (60-86400) (seconds)*:** A text input field.
- Task Description *:** A text input field.
- Task extern func:** A text input field.
- * Required:** A note indicating that fields marked with an asterisk are required.
- Submit** and **Reset** buttons at the bottom right.

To create a Health Monitor select the DSI Health Monitor object from the tree and execute the Create command. Use the definitions in the table below as a guide to configuring the fields in the Create Health Monitor interface (and then click the **Submit** button to save your configuration.

Use the **showStatusAll** operation at folder level for showing status of all health monitor tasks.

To update an existing Health Monitor object, select the DSI Health Monitor object from the tree, select the existing Health Monitor object from the list by checking the Select box and executing the Show command, make any necessary changes, and click the **Update** button to save the changes.

To check the status of each health monitor task, select the DSI Health Monitor object from the tree, select the existing Health Monitor object from the list by checking the **Select** box and executing the **Show Status** command.

DSI Health Monitor Fields Definition

Field	Definition
Name	The name of the Health Monitor task.
Type	The Type of the monitoring task. Select one of the following: • diskcap (Disk Capacity monitor) — To detect a disk usage threshold. • membrk (Process Memory monitor) — To detect a memory growth threshold for the process specified by the Task Description parameter. • corefile (Core File monitor) — To detect a threshold number of core files in /export/home/core. • logfile (Log File monitor) — To detect a change in size of the log file in /var/log/dsi. • workvulm (Work Volume monitor) — To collect performance statistics of the number of input CAM files and output files at a specified time interval. • commport (Communications Port monitor) — To detect the status of configured IP ports for DSI communications. • cfgdata (Configuration Data monitor) — To detect changes in DSI configuration data files and record them in the Health Monitor log. • userdef (User Defined monitor) — A user defined task with optional arguments defined in the Task Description parameter. • logkeep (Log File Maintenance monitor) — Maintains the Health Monitor log files for a specified number of days. • numfile (Directory Storage monitor) — Checks the number of files in the specified directory against a configured threshold. Generates an alarm when appropriate. • strandedfile — Stranded files monitor monitors files which remain in transporter client longer than expected • sourcefile — Source file monitor monitors the client for “idle time” threshold when there is no data. • appfile — App file monitor monitors the modification of binary or library files from last check
High Value	Specifies the threshold value to detect, when the task parameter is diskcap , membrk , corefile , or numfile .
Task Active	Enter a 1 (enabled) or 0 (disabled) to enable/disable this task.
Task Description	Specifies optional arguments of the task. For example, when the task parameter is membrk , this parameter specifies the process to be monitored, such as maintainer or tp. When the task parameter is diskcap , corefile , numfile , or logfile , this parameter specifies the absolute path to monitor (beginning with /). When the task parameter is userdef , this parameter specifies optional arguments to the user defined task specified in the Task Extern Func field.

Field	Definition
Task Extern Func	Specifies the executable or script to be run when the threshold value is met.

DSI Health Monitor Tasks

During the DSI installation, a default HMConfig file containing a set of predefined Health Monitor tasks is placed in /dsi/files. The table below provides the default settings for the predefined tasks.

Predefined DSI Health Monitor Task Settings

Name	Type	High Value	Task Active	Time Interval	Task Description	Extern Func
globaldisc	diskcap	50 95	1	600	/global/home/dsi	None
localdisc	diskcap	50 95	1	600	/export/home/dsi	None
maintainer	membrk	1 100	1	600	maintainer	None
tpmembrk	membrk	1 100	1	600	tp	None
corefile	corefile numfile	> 0 > 0	1	600	None	None
logfile	logfile	N/A (0)	1	600	/var/log/dsi	None
workflow	workvolm	N/A (0)	1	600	None	None
commport	commport	N/A (0)	1	600	None	None
cfgfile	cfgdata	N/A (0)	1	600	None	None
logkeep	logkeep	1 92	1	600	None	None
strandedfile	strandedfile	124	1	600	None	None
sourcefile	sourcefile	124	1	600	None	None
appfile	appfile	N/A	1	600	None	None

DSI Health Monitor Log

When the Health Monitor detects an anomaly, it logs it to the Health Monitor log. The Health Monitor logs consist of the configured logkeep number of daily log files functioning as a virtual circular log file. The logkeep number specifies the size of the virtual Health Monitor log file. The daily log file is created at midnight and is closed on the following midnight.

Note

For some anomalies, the Health Monitor raises an alarm to alert the operator to take appropriate action.

At startup time the Health Monitor checks the virtual log file and adjusts the number of the daily log files to the configured logkeep number. If no daily log file exists for that day, a new daily log file is created; otherwise, the system reopens the existing daily log file and appends new logs. The Health Monitor log files are located in /dsi/hm_log directory of the /global/home partition. Each log filename is prefixed with the host name, followed by the MM/DD/YYYY hh:mm:ss timestamp and with the hmlog file extension.

Note

Log messages generated from the user defined monitoring task are not written to the Health Monitor logs. They are logged in the `/var/log/dsi` directory.

To view a Health Monitor log file, select the DSI Health Monitor Log object from the tree, select the desired Health Monitor Log file from the list by checking the Select box and execute the **Show** command.

DSI Transporter Client

Additional articles:

- [Broadcast](#)
- [DSI Transporter Client Destination](#)
- [DSI Transporter Client Source](#)

The DSI Transporter Client section of the tree allows you to set the Fault Manager IP Address (**FM IP Address**) and the Fault Manager Port (**FM Port**) parameters. This section of the tree also provides access to the DSI Transporter Client Source and DSI Transporter Client Destination child objects. After making any changes, click the **Update** button to save your changes.

Note

After creating or changing any parameter in this section of the tree (including parameters associated with the child objects), you must use the Reload command from the DSI Transporter Client command list to enact the changes. The Reload command stops and restarts the Transporter processes.

Broadcast

The DSI Broadcast feature is a licensed feature which allows the DSI Transporter Client and Remote Client to specify any number of target destinations for a single source. If the Broadcast facility is enabled, files arriving at the source can be distributed to all target destinations. Usage of the Broadcast feature for more than two target

destinations requires a separate DSI feature license. Without this license, a user is allowed up to two targets per source.

If the broadcast license is not available, error/warning messages are shown when the user tries to add more than two hosts. These messages instruct the user to apply for the DSI Broadcast feature license.

Adding duplicate entries, that is, two destinations with the same IP address, also generates an error message.

DSI Transporter Client Destination

The parameters you specify in the DSI Transporter Client Destination object define a particular data exchange path that links a designated source directory on the local host (the NFS Server or the Customer Server) with a target directory on the remote host (DSI Server or Customer server). The system periodically collects and transfers file according to the configuration criteria. The following table provides the field definitions for the parameters associated with this object.

DSI Transporter Client Destination Field Definitions

Field	Definition
Name	The name for this Transporter session
Destination IP Address	The IP address of the remote host with which this session instance connects. Both the primary and secondary destination IP addresses support multiple comma separated values.
Destination Port	IP port of the remote host to be used by this session instance.
Destination Type	Choose either DSI for DSI Transporter Client, or 3RD for Transporter processes communicating with a Customer Server or Third Party. A Transporter Server connection type of 3RD restricts file system access by both: - Disallowing access above the working directory (login directory), as specified by the <code>working_dir</code> parameter of the client configuration entry - Disallowing directory modifications
Connection Type	Select one of the following: - Ftp regular FTP - SSLFtp SSLencrypted FTP - SFtp SSHencrypted FTP
Destination Directory (optional)	Indicates the location on the remote server where the system deposits the files.
Archive Source Files (optional)	If checked, after the successful transmission of the file to a remote server, the system moves the original file to the location specified in the archiveDir field. If unchecked, the system deletes the original file after transmission.
Archive Directory (optional)	Specifies the location where moves files following transmission, if archive flag is checked.
User Name	The Login ID used by the Client to login and establish a connection on the remote host.
Password	The password used by the Client to login and establish a connection on the remote host.
Source Directory	Specifies the directory to be watched for newly arriving files that are collected and transferred to the remote server.
Audit	Check box to enable or disable audit.

After making any changes, click the **Update** button to save your changes.

DSI Transporter Client Source

The parameters you define in the DSI Transporter Client Source object control how and when the system moves CAM files from the NFS server to the DSI server. The following figure and table provide the field definitions for the parameters associated with this object.

ID *:	
Data Source Name *:	
Data Source Type *:	GSX v
Delete CAM Records	☐
Source Directory *:	
Working Directory *:	
Destination Directory *:	
Archive Source Files	☐
Archive Directory:	
File Extension:	ACT
Filter ATTEMPT records	☐
Filter START records	☐
Filter STOP records	☐
Filter INTERMEDIATE records	☐
Filter REBOOT records	☐
Filter SWITCHOVER records	☐
Directory Scan Rate (0-3600) (seconds)	0
Duplicate Record Check Size (0-512) (bytes)	100
Max Records per File (0-):	0
Max Size per File (0-) (MB)	1
Max Time Period per File (0-) (seconds)	60
File Close Time (0-2400):	0
Broadcast	☐
Primary Destinations *:	
Secondary Destinations:	
* Required	
Submit Reset	

DSI Transporter Client Source Field Definitions

Field	Definition
ID	The unique ID for this set of parameters (64 character maximum).
Data Source Name	A reference name of the switch (64 character maximum). For example, gsx1dallas
Data Source Type	Select either the GSX or PSX as the switch type
Delete Cam Record	If checked, the system deletes the original CAM files following transmission. If unchecked, the system preserves the original CAM files. NOTE: If you check this box, then archiving will not occur regardless of the archive setting below
Source Directory	Defines the directory from which to collect original CAM files.
Working Directory	Defines the directory used to store temporary files.
Destination Directory	Defines the directory used to store the final billing files.
Archive Source Files (optional)	If checked, after the successful transmission of the file to a remote server, the system moves the original file to the location specified in the archiveDir field. If unchecked, the system deletes the original file after transmission.
Archive Directory (optional)	Specifies the location where the DSI moves files following transmission, if archive flag is checked.
File Extension (optional)	Defines the file extension of the original CAM files (default = ACT).
Filter Start Records (optional)	When checked, the Transporter filters out CAM records of type START.
Filter Stop Records (optional)	When checked, the Transporter filters out CAM records of type STOP.
Filter Intermediate Records (optional)	When checked, the Transporter filters out CAM records of type INTERMEDIATE.
Filter Reboot Records (optional)	When checked, the Transporter filters out CAM records of type REBOOT.
Filter Switchover Records (optional)	When checked, the Transporter filters out CAM records of type SWITCHOVER.

Field	Definition
Directory Scan Rate (optional)	Defines the time interval in seconds between directory scans to check for CAM data arrival. The valid range is between 0 and 3600 seconds with a default value of 1. Set the value to 0 (always) if heavy traffic is anticipated from GSX. NOTE: Although the default value for the Directory Scan Rate is 0, the preferred value is 1, because continuous scanning may cause the dsiCommClient process to consume a high percentage of the CPU resources. If a high traffic rate is anticipated, you can reset the value to 0.
Duplicate Record Check Size (optional)	This field defines the number of bytes used to review processed CAM records for possible duplicate records. The valid range is between 0 and 512 bytes with a default value of 100 bytes.
Max Records per File (optional)	Defines the record count threshold to promote the nonempty temporary billing file to the final billing file.
Max Size per File (optional)	Defines the time interval to promote the nonempty temporary billing file to the final billing file
Max Time Period per File (optional)	Defines the time of daily closing of the final billing file. The Transporter promotes the nonempty temporary file to the final billing file at this time of day regardless of other file closing criteria. The valid range is between 0 and 2400 with a default value of 0.
Broadcast	The check box is ticked if the broadcast feature is opted for.
Primary Destinations	A valid existing connection_name in the CommConfig file corresponding to the primary DSI host where billing files are to be transferred. The primary ID supports multiple comma separated destinations. When the DSI Broadcast feature is enabled, more than two target destination addresses can be specified.
Secondary Destinations (optional)	A valid existing connection_name in the CommConfig file corresponding to an alternative DSI host where billing files are to be transferred. The secondary ID supports multiple comma separated destinations.
Audit	Check box to enable or disable audit.

After making any changes, click the **Update** button to save your changes.

File Services

Additional articles:

- [File Services Sources](#)

File Services is a filter process providing basic file handling capabilities for those customers not needing the power of a DSI. The File Services feature individually filters files from GSX servers or other sources through a configurable set of processing steps and then places the files in output directories for forwarding to upstream systems. The **Show** command executes automatically, when you select the File Services object.

File Services Field Definitions

Field	Definition
Peer Port	The service port number on the host system. The valid range is between 5001 and 65535 with a default of 65535.
Peer Host	The name of the host system.
Directory Scan Rate	Defines the number of seconds between directory scans. The minimum period you can define is 5 seconds.
No File Activity	Defines the number of seconds before a single unchanging file, or a directory with no eligible files needs to be noticed. The minimum period you can define is 3600 seconds. The default is a setting of 0, which disables aging.
Filter 1 through 4	Used to designate filter/compression methods used on the source files. File Services uses the filters sequentially starting with Filter 1. Select the following file filtering/compression methods: • Checksum — Checksums a source file using standard Solaris Checksum utility (/usr/bin/cksum – CRC checksum) and appends the checksum value to the file. • Timestamp Rename — Manipulates the file name and timestamp of the file. If you designate multiple filters, then TimestampRename must be Filter 1. • Compress — Generates compressed files using compress (.Z file extension) • Gzip — Generates compressed files using gzip (.gz file extension) • None

After making any changes click the **Update** button to save your changes. To implement your changes immediately, use the **Reload** command.

File Services Sources

You can use the Sources child object of File Services to define the source and working directories for the File Services Feature, as well as the name of the system originating the files. The following table provides the field definitions for the parameters associated with this object.

File Services Source Field Definitions

Field	Definition
Name	The name of the system originating the files.
Source Directory	The path to the location that the originating system places the files.
Working Directory	The path to the directory that File Services uses as a temporary location to manipulate the files.

To create a new Sources object, select Create from the command list, enter values in the fields, and click the **Submit** button to save the object. To edit an existing object, select it from the list by checking the Select check box, make the necessary edits, and click the **Update** button to save your changes. To delete an existing object, select it from the list and execute the **Remove** command.

File Spec

A File Spec object defines the file sequence for output files by creating a particular instance of a File Template. While many fields are defined or defaulted based upon the File Template you select, you can edit several fields allowing for some level of customized behavior. To make use of a File Spec object, you associate it with an Output Connector object (see [Output Connector](#)).

To create a new File Spec object, select File Spec from the object tree and execute the **Create** command. To edit an existing object, select File Spec from the object tree, select the object from the list of existing objects, and execute the **Show** command.

File Spec Field Definitions

Field	Definition
Name	The name assigned to this File Spec object.
File Template	Specifies the output file format template to use: ama specifies standard AMA file naming convention. dsi specifies an existing file naming convention template to use. usr specifies a userdefined file naming convention template to use. fmt0 specifies the alternate format for AMAconnectors. It uses the same convention as the nonAMA standard filename: <DSI hostname>.<input filename>. <input_connector><output_connector>. <YYMMDDHHMMSS><4digit fileseqno>. out. fmt1 specifies filename convention: <10digit timestamp>.stream7.<4digit fileseqno>, where timestamp is time in seconds since 00:00:00 UTC, January 1, 1970. fmt2 specifies filename convention: <YYYYMMDD_HH:MM:SS><seqno[1..99999]>.csv. fmt3 specifies filename convention: <4digit fileseqno>.SONUS. fmt4 specifies filename convention: <YYYYMMDD_HH:MM:SS><seqno[1..99999]>.csv. fmt5 specifies filename convention: <string><4digit fileseqno>
Prefix	Specifies the prefix string used by this file specification.
Suffix	Specifies the suffix string used by this file specification.
Startup Init	Specifies the initial value to use for the sequence number. this value must be between the minimum and maximum.
Reset Timer	Specifies the interval/time at which to reset the sequence number. The entry must conform to the following syntax: minutes (0 to 59), hour of day (0 to 23), day of month (1 to 31), month of year (1 to 12), and day of week (0 to 6, where 0 is Sunday). Separate each field entry with a space and multiple entries in a field by a comma. You may specify a range of values in a field by using a dash. An asterisk in any field signifies all valid values. For example, an entry of <code>15 3 * * *</code> would result in the system force closing the files at 3:15 AM every day of every month. or <code>30 0,12 * * 15</code> would result in the system force closing the files at 12:30 AM and 12:30 PM, Monday through Friday. An entry of “—” (without quotes) disables the argument. This setting applies to the AMA template only.

Field	Definition
Tracer Timer	Specifies the interval/time at which to generate a tracer record. The entry must conform to the following syntax: minutes (0 to 59), hour of day (0 to 23), day of month (1 to 31), month of year (1 to 12), and day of week (0 to 6, where 0 is Sunday). Separate each field entry with a space and multiple entries in a field by a comma. You may specify a range of values in a field by using a dash. An asterisk in any field signifies all valid values. For example, an entry of 15 3 * * * would result in the system force closing the files at 3:15 AM every day of every month. or 30 0,12 * * 15 would result in the system force closing the files at 12:30 AM and 12:30 PM, Monday through Friday. An entry of “—” (without quotes) disables the argument.
Generate S/W Change Record	Specifies whether or not to generate a software change record. The default value is checked (generate change record).
Track to FTP Status File	Specifies whether or not to log changes in a status file through FTP push mechanism (which must be active). The default value is checked (log changes).
Minimum	Specifies the minimum value of sequence records used by this file specification.
Maximum	Specifies the maximum value of sequence records used by this file specification.
Current	Specifies the current value of sequence records used by this file specification

To save a new File Spec object or too save the changes to an existing object, click either the **Submit** or **Update** button as appropriate.

File Template

The File Template object allows you to access the settings for the various File Formats used by the File Spec object. You cannot create new template or edit the prepackaged templates included with the DSI installation. To see the setting associated wit a File Template object, select the File Template object from the object tree, select the template you wish to view from the list, and execute the Show command. The fields displayed for each template are defined in the table below.

File Template Field Definitions

Field	Definition
File Template Name	The name assigned to this File Template object.
File Template Description	Provides a brief description of this template.
File Template Format Name	The name for this format.
File Template File Format	The format for this file.
File Template Prefix	Specifies the prefix string used by this file template.
File Template Suffix	Specifies the suffix string used by this file template.
Minimum	Specifies the minimum value of sequence records used by this file specification.
Maximum	Specifies the maximum value of sequence records used by this file specification.
Init at Start	Specifies whether defining an initial sequence start value is allowed.
Reset at Start	Specifies whether resetting at start is allowed.
Reset at Interval	Specifies whether resetting at an interval is allowed.
File Build Function	Specifies the function used to build a file name.
Tracer Record at Interval	Specifies whether the Tracer record creation at defined intervals is configured for this template.
S/W Change Record	Specifies whether or not the software change record generation is configured for this template.
S/W Change Record	Specifies whether or not to log changes in a status file through FTP push mechanism (which must be active). The default value is checked (log changes).
Is Sequence Used	Defines whether or not the sequence is used.

FTP Client

The FTP Client category of the DSI Manager object tree allows you to signal the DSI to manually push all files in the ftp push daemon's queue to the primary ftp destination. To do this, select the FTP Client category in the object tree and select **Push Files Manually** from the command list.

The Show command displays the parameters listed in the table below, which control the push operation. If you change any of the parameter values, click the **Update** button to save you changes.

FTP Client Field Definitions

Retry Wait Time	Specifies the number of seconds FTP Push waits before attempting another retry. The default is 30 seconds.
Max Consecutive Retries	Specifies the number of FTP Push retries before a file is considered failed. The default is 3.
Push Criteria Value	Specifies, in conjunction with the Push Criteria Type entry, the method used and the frequency that the DSI pushes files to the remote system. If you set the Push Criteria Type to Cron, enter a positive integer (or series of integers separated by commas) representing the number of minutes past the hour that the DSI pushes the files. For example, to push files every 10 minutes type: 0,10,20,30,40,50 * * * * If you set the Push Criteria Type to Number of Files, enter a positive integer representing the number of files to accumulate before the files are pushed. If you set the Push Criteria Type to Period enter the number of seconds that should elapse before the DSI pushes the files. For example, enter 300 to indicate an elapsed time of 5 minutes between pushes.
Push Criteria Type	Specifies, in conjunction with the Push Criteria Value entry, the method the DSI uses to push files to the remote system. Valid entries are: • Number of Files • Cron • Period

FTP Daemon

Selecting the FTP Daemon category automatically executes the Show command allowing you to set two controls that enable/disable the use of passive FTP and the renaming of primary files during an FTP pull operation. The following table defines these controls.

FTP Daemon Field Definitions

Field	Definition
Enable Passive FTP	If checked, the system allows the use of a passive FTP connection.
Rename Files	If checked, the system will expect a manual file rename on an FTP pull operation. If unchecked, the system automatically renames the file on an FTP pull operation. Default is unchecked.

If you change any of the parameter values, click the **Update** button to save you changes.

IMDS

The DSI provides support for an IMDS mediation system by acting as a billing record server used by the IMDS to retrieve (through FTP polling) consolidated CDR records collected from various GSXs. A CDR merging process consolidates the processed CDR records and packages the records into a CDR file following the IMDSprescribed data slot format.

The CDR file name is in the form of <prefix>_<sequence number>.<suffix> where:

<prefix> is a text string in the form of DSIxxy, where xx is the DSI cluster ID number and y is the Directory ID. Both the DSI cluster ID number and the Directory ID are configurable.

<sequence number> is a 6digit number (range: 000000 999999), to guarantee a unique file name. When the sequence number reaches 999999, the next sequence number is reset back to 000000.

<suffix> is a configurable string as the file extension.

Executing the **Show** command displays the Update IDMS interface. After changing any of the parameter settings, click the **Update** button to save your changes. Use the definitions in the table as a guide to the parameters.

Update IMDS Interface

Cluster ID * :	00
CDR Storage Directory ID * :	0
IMDS interface version * :	0
Suffix of the CDR file name * :	cdr
Max CDR Count (5000-50000) * :	10000
Max File Size (1024-16384) * :	2048
Max CDR Timeout (10-180) * :	30
Max File Timeout (60-600) * :	300
Daily File Close (0000-2400) * :	2400
Time Since Generation (96-240) * :	96
Keep Time Post (48-120) * :	48

* Required

Update IMDS Field Definition

Field	Definition
Cluster ID	Defines the Cluster ID for the IMDS interface. The valid range is between 0 and 99. The default value is 00.
CDR Storage Directory ID	Defines the CDR Storage Directory ID for the IMDS interface. The valid range is between 0 and 9. The default value is 0.
IMDS Interface Version	Defines the version of the IMDS interface. The default value is 0.
CDR Filename Suffix	Defines the suffix used for the CDR filename. The default value is cdr.
NOTE: The limits specified in the following five parameters have a logical OR relationship. If any individual limit is exceeded, the CDR file closes.	
Max CDR Count	Defines the maximum number of CDR records included per CDR file. The valid range is between 5000 and 50000 files with a default value of 10000 records.

Field	Definition
Max File Size	Defines the maximum size of the CDR file in kilobytes. The valid range is between 1024 KB and 16384 KB with a default value of 2048 KB.
Max CDR Timeout	Defines the maximum CDR record writing idle time in seconds for closing the CDR file. The valid range is between 10 seconds and 180 seconds with a default value of 30 seconds.
Max File Timeout	Defines the maximum allowed CDR file opening duration in seconds. The valid range is between 60 seconds and 600 seconds with a default value of 300 seconds.
Daily File Close	Defines the CDR daily closing time in military format with a default value of 2400 (midnight) and a value of 0000 disabling the parameter.
Time Since Generation	Defines the amount of time in hours after file generation that the system retains the CDR file. The valid range is between 96 hours and 240 hours with a default value of 96 hours.
Keep Time Posted	Defines the amount of time in hours after file archiving that the system retains the CDR file. The valid range is between 48 hours and 120 hours with a default value of 48 hours.

In addition to the Show command, there are several other commands available after selecting the IMDS object from the tree. The table below provides information concerning these commands.

IMDS Commands

Command	Function
Perform DAT Transfer	Initiates a DAT transfer request to tar CDR files. Use this command when you want to offload the CDR files to another storage space (for example, in the event of loss of connection between DSI and the IMDS server when realtime transfer is not possible).
Show All GSX Stats	The system displays the following GSX/IDMS statistics for all GSXs serviced by this DSI: • Number of CAM files received • Number of CDR records written to CDR files

Command	Function
Show CDR Stats	After supplying the CDR number and clicking the Submit button, the system displays the following statistics: • Number of CDR records in the specified CDR file • Status of the specified CDR file (Transferred or Nottransferred)
Show DSI Stats	Displays the following DSI IMDS related statistics: • Number of GSX CAM files received by DSI • Number of CDR records generated by DSI • Number of CDR files generated by DSI • Number of CDR files transferred to IMDS • Number of CDR files waiting to be transferred to IMDS
Show GSX Stats	After supplying the name of the GSX and clicking the Submit button, the system displays the following statistics: • Number of CAM files received • Number of CDR records written to CDR files
Clear DSI Stats	Clears the DSI IMDS related statistics.
Clear GSX Stats	After supplying the name of the GSX and clicking the Submit button, the system resets the GSX/IDMS related statistics.

Input Connector

To create a new Input Connector, select Create from the command list and complete the fields using the definitions in the table below as a guide. After entering the necessary information, click the **Submit** button to save the new object.

Create Input Connector Field Definitions

Field	Definition
Input Configuration File	Points to the <input_name>_config file in the /dsi/config directory determining which configuration file the DataStream Integrator uses. The maximum field length is 32 characters.
DLL	The name used to register the connector so the DataStream Integrator knows which processing path to take.
Address	When using the TCP protocol, this field defines either the hostname or the IP address of the external system.
Protocol	Identifies the network protocol used to transmit data through the communication port. Possible values are: • ama_file • db • file • stdio • tcp • udp
Port	When using the TCP protocol, this field defines the unique TCP port number. If you use either file or ama_file protocol, you can use this field to define a specific file to be processed at the time specified by the timer field. This is an optional field when the protocol is file or ama_file and there is no timer string

Field	Definition
Options	This field contains a group of three switches (either a 0 or a 1) that define system actions with regard to incoming error messages. The first switch determines whether this connector expects to receive external system connections (listening). This listening option applies only to the TCP protocol of an input Adaptor. The switch definitions are: • 0 the connector does not expect input data • 1 the connector expects input data The second switch determines whether the system should wait for a response to messages it sent before ending the session. This response option applies only to the TCP protocol. The switch definitions are: • 0 the system does not wait for a response to a sent message • 1 the system does wait for a response to a sent message The third switch, the batch scanner option, determines whether the system scans for files in the designated dropbox directory. The batch scanner option applies only to the file or ama_file protocol. The switch definitions are: • 0 the system does not scan for files in the dropbox directory • 1 the system scans for files in the dropbox directory at specified intervals. The DataStream Integrator creates a dropbox directory for the placement of input data files. The Batch.Files.Directory entry in dsi_config determines the location of the input (drop box), output, and archive subdirectories for batch processing. If you used the default installation settings, this entry will be /dsi/batchfiles/<Adaptor_name_instance>. Examples: A value of 100 means that DataStream Integrator listens for incoming data messages at the specified address and port. A value of 001 means that DataStream Integrator will scan the designated dropbox directory for files to be processed.
Timer String	This field contains a string formatted to conform to the Unix cron command, which defines when the DataStream Integrator starts a job. For example, 30**** means to start a job on the halfhour of every hour of every day of every month.
Input Timeout	The number of seconds during which the DataStream Integrator either attempts to start a job, or if there is idle time during the transmission of data, waits before disconnecting. The DataStream Integrator retries the job every 5 seconds for the specified number of seconds.
Max Output Queue Size	This field controls the internal message flow by defining the maximum number of messages that can be waiting for processing. The number of messages waiting must be below this limit before the system accepts the next input message.

Field	Definition
Priority	Indicates the relative precedence this job has within a queue of jobs. If two jobs arrive at the same time, the system process the one with the higher priority first.
Sensor ID	A unique 6digit code identifying the system that generates and/or formats the AMA record. This information appears in tracer records where you create an hourly tracer for each generating system. (maximum value = 999999)
Sensor Type	This is a 3digit code that identifies the type of system that generates and/or formats the AMA record. (maximum value = 999, default = 199)
Name	A unique name designating the Input Connector instance. The maximum field length is 32 characters.

To edit an existing Input Connector object, select it from the list by checking the **Select** box next to the object name and execute the **Show** command. After changing any of the parameter values, click the **Update** button to save you changes.

To delete a Input Connector object, select it from the list by checking the Select box next to the object name and execute the **Remove** command.

Each Input Connector object has three child objects, Archive Record, Input Record, and Source Record which hold individual record files. Selecting a record from the list by checking the Select box next to the object name and executing the **Convert** command displays the record in readable format in a new window.

Load Balancer Configuration

You can use the Load Balancer object to provision load distribution (balancing) policies. The available options are:

- **RoundRobin** — Data files received by a DSI cluster are distributed to individual nodes in a round robin fashion (sequentially).
- **WeightedRoundRobin** — Data files received by a DSI cluster are distributed to individual nodes in a round robin fashion with weight given based on the number of CPUs in a particular node.
- **LeastLoaded** — Data files received by the DSI cluster are distributed to the least loaded node in the cluster, based on factors such as number of processors, assigned node weight, CPU load averages, and job queue size.

If you change the Load Balancer policy, click the **Update** button to save you changes.

Using the **Set Load Balancer Weight** command you can also provision the load balancing weight for a specified node in a cluster by selecting the node and entering a **Weight** value for the selected node. Weight represents the percentage of batch files to be assigned to the node. The sum of all weights for all nodes in the cluster must equal 100. After entering/changing any of the parameter values, click either the **Submit** or **Update** button, as appropriate, to save you changes.

Maintainer

Additional articles:

- [House Keeping](#)

One of the three main components of Data Stream Integrator, the Maintainer manages the batch system components, and performs scheduled House Keeping tasks. The batch system is made up of two components:

- The scanner scans the dropbox directory. When an input file appears in one of the drop box's subdirectories, the Maintainer transfers it for batch processing.
- The batch process manager starts and stops batch jobs. When the scanner submits a batch job to the maintainer, the batch process manager component of the Maintainer transfers the job to the Transaction Processor (TP) and monitors it to completion.

Clicking on the Maintainer category automatically displays the results of a Show command. From this interface you can set three parameters that control the operation of the scanner and batch processing functions. The following table defines these parameters.

Maintainer Show Field Definitions

Field	Definition
Scan Period	Specifies the number of seconds that the system waits between each scan of dropbox directories. When the scanner detects a file whose size has not changed since the last scan, it begins processing the file. The entered value must be between 5 and 600 seconds. The default setting is 10 seconds. If you change the value of Scan Period, you must reload DataStream Integrator. Reloading DataStream Integrator does not affect processing.
Input Retries	Specifies number of times the Maintainer process retries a failed input file before halting the job. The specified entry must be between 1 and 20. Default is 1.
NOTE: The Transaction Processor tries each file submitted by the Maintainer a maximum of five times.	
Archive Files	If checked, the system archives CAM files. Default is checked.

If you change any of the parameter values, click the **Update** button to save you changes.

House Keeping

The House Keeping subcategory under the maintainer allows you to create and delete tasks in the housekeeping file. The housekeeping file contains the parameters used to determine the method and timing for routine cleanup of files contained in the archive or output directory associated with a particular Adaptor instance. The House Keeping subcategory contains a listing (tree) of the tasks that you have added to the housekeeping file. Clicking on a task name performs a **Show** command and displays the parameters for the task. You can edit the House Keeping parameters (see the table below) from this display.

Selecting **Remove** from the command list deletes the selected task from the file.

Note

There is no confirmation message associated with the delete command. Verify that you have selected the correct task you wish to delete prior to executing the command.

To create a new task, select **Create** from the command list and complete the fields using the definitions in the following table as a guide.

House Keeping Create/Update Field Definitions

Field	Definition
Age	Specifies the maximum number of days a file can remain in an archive or output directory associated with the Adaptor instance. The housekeeping task removes files older than this setting.
Min File Size	Specifies the maximum file size in bytes for files in the archive or output directory associated with the Adaptor instance. The housekeeping task removes files larger than this setting.
Number of Files	Specifies the maximum number of files allowed to accumulate in the archive or output directory associated with the Adaptor instance. The housekeeping task removes excess files on a first in first out basis until the number of files falls below the specified limit.
Function	Defines the functions provided by the DSI that run during the timer specified in the housekeeping jobs to accommodate the in memory correlation feature. There are no user defined functions associated with this field.
Function Arguments	Provides arguments to the function specified in the function field. There are no user defined functions associated with this field.
Timer String	Specifies the times (times, days, and dates) for the system to run the housekeeping task. The entry must conform to the following syntax: minutes (0 to 59), hour of day (0 to 23), day of month (1 to 31), month of year (1 to 12), and day of week (0 to 6, where 0 is Sunday). Separate each field entry with a space and multiple entries in a field by a comma. You may specify a range of values in a field by using a dash. An asterisk in any field signifies all valid values. For example, an entry of 15 3 * * * would result in the housekeeping task running at 3:15 AM every day of every month. or 30 0,12 * * 15 would result in the housekeeping task running at 12:30 AM and 12:30 PM, Monday through Friday.
Name	A unique name designating the Housekeeping Task. The maximum field length is 32 characters.
Type	Select one of the following options that define the type of Housekeeping operation: • scalable — executes the Housekeeping job on all nodes in the cluster • failover — executes the Housekeeping job on only a single master node in the cluster

MATS BE Server

Additional articles:

- [AMA File](#)
- [AMA File Closing Schedules](#)

The MATS Server category contains commands and child objects (AMA File Closing Schedule and AMA File) used to control the realtime and Batch transfer interface for moving AMA files between the DSI and the MATS Billing System. The following table provides definitions for the commands available for the MATS Server object.

MATS BE Server Commands

Command	Definition
Show	Displays the status of the MATS connection and the Real Time Transfer State in the form of: Connection link status, Cause, Real time transfer status, Cause . For example, UP, , START, or DOWN (Activation request for DSIM in progress?, No response from MATS
Start Real Time Transfer	Starts (or resumes) the real time transfer of AMA files to the MATS server.
Stop Real Time Transfer	Stops (or suspends) the real time transfer of AMA files to the MATS server.
Close Current File Now	Closes the current AMA file. You can use this command to manually close the current AMA file prior to the scheduled automatic close time. The system returns one of two results: • Success — The DSI closed the file successfully • Rejected — The DSI could not close the file successfully. This result typically occurs if you issue the command while the system is already closing the file per the scheduled close time.
NOTE: In addition to the scheduled close times, the DSI also closes AMA files upon reaching the 64 sub-file limit.	

Command	Definition
DAT Transfer	Initiates the tarring of the specified file(s). The argument for this command is a regular expression, <code>nnn[,nnn*] nnnnnn</code>, where <code>nnn</code> is the ama number from 000 to 255. To specify multiple nonconsecutive ama numbers use a comma as delimiter. For example, 000,125,232 would result in the tarring of ama files 000, 125, and 232. To specify a range of consecutive ama numbers use a hyphen between two ama numbers indicating the lower and upper limits of the desired range. For example, 000032 would result in the tarring of ama all files between 000 and 032 inclusive. The system returns one of two results: • Success — The DSI created the tar file successfully • Rejected — The DSI could not create the tar file. This result typically occurs if you a file that is still open or in the process of being transferred. The DSI stores the generated tar file(s) in the MATS/DAT directory using a filename in the format: ama<xxx>.yymmddhhmm, where <code><xxx></code> is the ama number and <code>yymmddhhmm</code> is the timestamp.

AMA File

The AMA File object acts as a holding area for the DSI created MATS AMA files. To show information for a particular AMA file, select it from the list. The system automatically run a Show command displaying the following information:

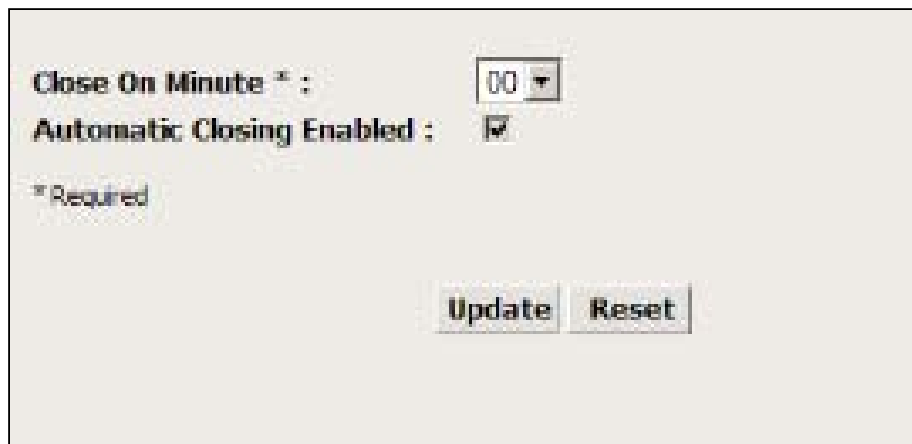
File Name the name of the selected AMA file in the form of `amaNNN`, where `NNN` is the ama number from 000 to 255

- **Starting Sub File** — The name of the first CDR file added to the AMA file
- **Ending Sub File** — The name of the last CDR file added to the AMA file
- **Sub Files Count** — The number of CDR files added to the AMA file. The DSI also closes AMA files upon reaching the 64 subfile limit.
- **Status** — The status of the AMA file (either open or closed)
- **Created Time** — The time the AMA file was created
- **Closed Time** — The time the AMA file was closed (blank if Status = open)
- **Transfer Status** — The status of the transfer of the AMA file to the MATS Server (either Waiting, In Process, Completed, or Suspended)
- **Transfer Time** — The time that the transfer of the AMA file to the MATS Server completed.

AMA File Closing Schedules

The AMA File Closing Schedules object allows you to schedule automatic closing of the AMA files. Initially, this object contains 24 child objects numbered 00 through 23 representing the hours from 12:00 AM through 11:00 PM with automatic AMA file closings schedule at the top of each hour. By selecting an individual (hour) object you can disable a scheduled closing completely or change the timing in 10 minute increments; thereby adjusting the AMA file closing intervals based upon anticipated traffic volume.

AMA File Closing Schedule Interface



The screenshot shows a configuration panel with a light gray background. At the top, the text "Close On Minute ^{*}:" is followed by a dropdown menu showing "00" with a downward arrow. Below this, the text "Automatic Closing Enabled:" is followed by a checked checkbox. At the bottom left, there is a small text label "^{*} Required". At the bottom center, there are two buttons: "Update" and "Reset".

To disable a particular scheduled closing, select the (hour) object, uncheck the **Automatic Closing Enabled** check box, and click the **Update** button. The change takes effect at the next scheduled closing.

To change the timing of a scheduled closing, select the (hour) object, select a new **Close on Minute** setting (00,10,20,30,40, or 50 minutes past the hour), and click the **Update** button. The change takes effect at the next scheduled closing.

Operating Modes

The available Operating Modes of the DSI are determined as a function of the feature licenses enabled and the various runtime profiles within those licensed features. This tree object provided the ability to examine (**Show** command) the current Operating Mode settings and to toggle each Operating Mode of the DSI (depending on licensing) on and off. The table below provides information concerning the available commands and the associated required license levels.

Operating Mode Options

Command	License Required	Description
BCAM Reception	L0	Enables or disables binary CAM reception from a GSX client.
BCAM to ASCII CAM	L0	Enables or disables binary CAM conversion to legacy ASCII CAM format. Note: This operating mode also requires operating mode 1 to be enabled. (See note below.)
Transporter Client Services	L0	Enables or disables the DSI Transporter Client service. This service is intended to enable one DSI/NFS instance operating in “NFS” mode to send CAM data to another DSI/NFS instance operating in “DSI” mode.
File Services	L1	Enables or disables the File Services features and services associated with L1.
DSI Services	L2	Enables or disables the DSI features and services associated with L2.
IMDS Services	L2	Enables or disables the DSI IMDS related features and services.

After making any changes click the **Update** button to save your changes.

Note

To use the BCAM to ASCII CAM command you must supply an authorized User Name and Password separate from the EMS log in information. This requires the creation of special Access Control File by Ribbon. Consult your Ribbon representative for additional information. All other Operating Mode commands are available to anyone having access to DSI Manager.

Output Connector

To create a new Output Connector, select Create from the command list and complete the fields using the definitions in the table as a guide. After entering the necessary information, click the **Submit** button to save the new object.

Create Output Connector Field Definitions

Field	Definition
Output Configuration File	Points to the <output_name>_config file in the /dsi/config directory determining which configuration file the DataStream Integrator uses. The maximum field length is 32 characters.
DLL	The name used to register the connector so the DataStream Integrator knows which processing path to take.
Address	When using the TCP protocol, this field defines either the hostname or the IP address of the external system.
Protocol	Identifies the network protocol used to transmit data through the communication port. Possible values are: • ama_file • db • file • stdio • tcp • udp
Port	When using the TCP protocol, this field defines the unique TCP port number. If you use either file or ama_file protocol, you can use this field to define a specific file to be processed at the time specified by the timer field. This is an optional field when the protocol is file or ama_file and there is no timer string.

Field	Definition
Options	This field contains a group of three switches (either a 0 or a 1) that define system actions with regard to incoming error messages. The first switch determines whether this connector expects to receive external system connections (listening). This listening option applies only to the TCP protocol of an input Adaptor. The switch definitions are: • 0 the connector does not expect input data • 1 the connector expects input data The second switch determines whether the system should wait for a response to messages it sent before ending the session. This response option applies only to the TCP protocol of an input Adaptor. The switch definitions are: • 0 the system does not wait for a response to a sent message • 1 the system does wait for a response to a sent message The third switch, the batch scanner option, determines whether the system scans for files in the designated dropbox directory. The batch scanner option applies only to the file or ama_file protocol. The switch definitions are: • 0 the system does not scan for files in the dropbox directory • 1 the system scans for files in the dropbox directory at specified intervals. The DataStream Integrator creates a dropbox directory for the placement of input data files. The Batch.Files.Directory entry in dsi_config determines the location of the input (drop box), output, and archive subdirectories for batch processing. If you used the default installation settings, this entry will be /dsi/batchfiles/<Adaptor_name_instance>. Examples: A value of 100 means that DataStream Integrator listens for incoming data messages at the specified address and port. A value of 001 means that DataStream Integrator will scan the designated dropbox directory for files to be processed
Linked Definition	Contains a connector ID that receives the output of the connector currently defined as its input. For example, you can define the output of connector 5 to be the input of connector 1. This will trigger a new job in connector 1. The protocols of both connectors must match. If the connector identified in the Linked Definition field uses the TCP protocol, then the originating connector must also use the TCP protocol
Max Output Queue Size	This field controls the internal message flow by defining the maximum number of messages that can be waiting for processing. The number of messages waiting must be below this limit before the system accepts the next input message.

Field	Definition
Priority	Indicates the relative precedence this job has within a queue of jobs. If two jobs arrive at the same time, the system process the one with the higher priority first.
Sensor ID	A unique 6digit code identifying the system that generates and/or formats the AMA record. This information appears in tracer records where you create an hourly tracer for each generating system. (maximum value = 999999)
Sensor Type	This is a 3digit code that identifies the type of system that generates and/or formats the AMA record. (maximum value = 999, default = 199)
Both the Sensor ID and Sensor Type fields are required for AMA records.	
Name	A unique name designating the Output Connector instance. The maximum field length is 32 characters.
RSN Spec	Specifies a record sequence numbering specification to associate with this Output Connector definition. The absence of a record sequence numbering specification disables Record Sequence Numbering of the output records.
File Spec	Specifies a file sequence naming specification to associate with this Output Connector definition. The presence of file sequence naming specification overrides the global file format available to sequence the output files.
Closure Spec	Defines the Closure Spec object to be associated with this Output Connector object. The absence of file closure specification disables output consolidation.
Destination Directory	Specifies either a destination directory to associate with this Output Connector definition or the directory that can be derived from the connector definition: • If you enter a Destination Directory, the DSI uses the specified directory as the final dropbox for output files. If the specified directory does not exist, DSI runtime attempts to create the directory. • In the absence of the connector definition, the DSI uses the default connectordefinitionderived directory as the final dropbox for output files. • If you leave the Destination Directory field blank, the destination directory from the connector definition is preferred before considering the default connectordefinitionderived directory.

To edit an existing Output Connector object, select it from the list by checking the **Select** box next to the object name and execute the **Show** command. After changing any of the parameter values, click the **Update** button to save you changes.

To delete a Output Connector object, select it from the list by checking the Select box next to the object name and execute the **Remove** command.

Package

The Package category provides information concerning the version numbers of the various packages available for installation on your DSI. To install a package, expand the tree to display the Package Name and the Package Adaptor child object. Select the package from the list by checking the Select check box and execute the **Install Adaptor** from the Command list. There is also a **Show** command available that displays version information.

Ports

The Ports category allows you to enable/disable the ports used for ftp and telnet connections, as well as the port numbers. Selecting the Ports category displays the current settings for **AMA FTP Port**, **Standard FTP Port**, **Standard Telnet Port**, and **AMA Telnet Port**. To change the port number(s), simply change the value shown. To enable/disable a port change the state of the check box below the port setting. After making any changes click the **Update** button to save your changes.

Route Definition

You can use the Route Definition category to create, delete, or edit entries to the Route Definition file. The Route Definition file records the routes between input and output adaptor instances.

To create a new Route Definition, select Create from the command list and complete the fields using the definitions in the table below as a guide. After entering the necessary information, click the **Submit** button to save the new object.

Create Route Definition Field Definitions

Field	Definition
Output Connector	The name of the output connector used to convert the data received from the input connector.
Input Connector	The name of the input connector.
Expect Response	Determines whether or not the DataStream Integrator internally returns a response message from the destination host. If checked a response is sent and the DataStream Integrator prevents the input session from shutting down until it has processed all of the expected response messages. If unchecked (default) then no response is sent. You can use this option only for connectors that use TCP as a protocol.

To edit an existing Route Definition object, select it from the list by checking the **Select** box next to the object name and execute the **Show** command. After changing any of the parameter values, click the **Update** button to save you changes.

Note

If either the Input Connector or Output Connector referenced by the Route Definition has been deleted, you will receive an error message when executing the Show command on the Route Definition object.

To delete a Route Definition object, select it from the list by checking the Select box next to the object name and execute the **Remove** command.

RSN Sequence

You use the RSN Sequence object to define record sequence numbering specifications used by the DSI.

To create a new RSN Sequence, select Create from the command list and complete the fields using the definitions in the table below as a guide. After entering the necessary information, click the Submit button to save the new object.

RSN Sequence Field Definitions

Field	Definition
Name	The name of this RSN Sequence object.
Minimum	Defines the minimum value of sequence records in the output CDR file.
Current	Specifies the starting sequence number.
Maximum	Defines the maximum value of sequence records in the output CDR file. When this value is reached, the output CDR file is closed and a new file started, with sequence numbering restarted.
Concurrent	A check indicates the use of the sequence concurrently. If uncheck, it indicates the use of the sequence sequentially.

To edit an existing RSN Sequence object, select it from the list by checking the **Select** box next to the object name and execute the **Show** command. After changing any of the parameter values, click the **Update** button to save you changes.

RSN Spec

The RSN Spec object defines the record sequence field placeholder in a given record. Since the parameters can vary for different adaptors, each of the connector objects can have their private RSN Spec object associated.

To create a new RSN Spec, select Create from the command list and complete the fields using the definitions in table below as a guide. After entering the necessary information, click the **Submit** button to save the new object.

RSN Spec Field Definitions

Field	Definition
Name	The name of this RSN Spec object.
Sequence Start	Defines the offset of the sequence field from the beginning of the record: • fixed=+ve integer value in bits. Use when all the records that can appear in the output files require the sequence field to appear at a fixed offset from the beginning of the record. • delim=(recname:0x<delimiter value in hex>:count[:pattern]),*. Use when records have delimited fields with varying sequence field order. Enumerate the individual records with recordname, field delimiter token, sequence field number order, and optional pattern to verify in that field before stamping the sequence number. Separate each tuple by a comma. • pattern=pattern. Use for all other kinds of record cases. Specify a pattern, the first instance of which should be replaced with the sequence number.
Sequence Size	Defines the allowed occupancy size of the record sequence.
Sequence Format	Specifies the printable representation of the record sequence onto the record. The possible selections are: binary, ascii, hex, or nibble.
Record Delimiter	Defines the delimiter used to Identify the record end. • delim=0x delimiter value in hex. Use for a variable record. • fixed=+ve integer recordsize in bits. Use for a fixedsize record. • TLVi=recordsize length in bits. Use for a TagLengthValued record inclusive of TLV bytes. The acceptable range for bit length is between 4 and 32 bits. • TLVx=recordsize length in bits. Use for a TagLengthValued record exclusive of TLV bytes. The acceptable range for bit length is between 4 and 32 bits.

Field	Definition
Sequence Reset	Specifies the interval/time at which to reset the sequence number. The entry must conform to the following syntax: minutes (0 to 59), hour of day (0 to 23), day of month (1 to 31), month of year (1 to 12), and day of week (0 to 6, where 0 is Sunday). Separate each field entry with a space and multiple entries in a field by a comma. You may specify a range of values in a field by using a dash. An asterisk in any field signifies all valid values. For example, an entry of 15 3 * * * would result in the system force closing the files at 3:15 AM every day of every month. or 30 0,12 * * 15 would result in the system force closing the files at 12:30 AM and 12:30 PM, Monday through Friday. An entry of “—” (without quotes) disables the argument. Note: The Sequence Reset setting of the Closure Spec object takes precedence over this setting.
Exposure	Specifies the usage of this record specification: • local — specifies the record specification is associated with only one connector object. • global — specifies the record specification is associated with any number of connector objects.
LnkRsnSequencePK	Specifies the link to a userdefined data set.
Sequence Properties	Specifies the sequence setting specified at configuration time.

To edit an existing RSN Spec object, select it from the list by checking the **Select** box next to the object name and execute the **Show** command. After changing any of the parameter values, click the **Update** button to save you changes.

Stream Configuration

The Stream Configuration section of the tree allows you to create Stream Configurations objects that map input streams from Stream Clients to the receiving Stream Server and associated Transaction Processors. To create new Stream Configuration object select the Create command and complete the fields using the definitions in the table below as a guide.

You can update existing Stream Configuration objects by selecting an object from the tree, changing the applicable parameters and then clicking the **Update** button. You can delete an object by selecting it and then selecting the **Delete** command from the command list. There are also two additional commands that allow you to display (**Show Stats**) or reset (**Reset Stats**) statistics associated with the selected object.

Create/Update Stream Configuration Interface Field Definitions

Field	Definition
Node Name (read Only on Update)	The name of this configuration entry. NOTE: The trap resync for GSX device functions only when the GSX name given in the EMS Insight administration and the stream name configured on the DSI are same.
Active (optional)	Enables (checked) or disables (unchecked) this Stream Configuration.
Out Port (optional)	The port to which the Stream Server writes data. The valid range is between 5001 and 65535.
Source IP Address 1 through 8 (2 through 7 are optional)	The IP address of the Stream Client. You can configure up to 8 addresses.
User ID	The Stream Clients User ID used to log on to the Stream Server.
Password	The password associated with the User ID.
Data Directory (Read Only)	The stream buffer directory used to store the BCAM file. (default = /dsi/dirData)
Log Directory (Read Only)	The directory used to store the Event Log file. (default = /dsi/dirEventLog)
Output Connector Name (optional)	The name of the Output Connector used for BCAM processing.
BPA IP Address (optional)	The IP Address of the BPA Server.
BPA Port (optional)	The IP Port of the BPA Server.
Backend Server Selector	The type of Backend Server. Select between None , SAI , or MAT .
Max Records per File	Defines the maximum number of billing records per file.
Billing Rollover Time	Defines the time interval for rolling over the billing record file.
Billing File Size	Defines the maximum size of the billing record file.
BCAM Rollover Time	Defines the time to rollover the BCAM file on a daily basis.

Field	Definition
Event Log File Size	Defines the maximum size of the Event Log file. (default = 2000000 = 2MB)
Maximum Logs	Defines the maximum of log files to keep. (default = 32)
Reconnect Attempts	Defines the number of time to attempt reconnection. The valid range is between 1 and 60, with a default of 60.
Reconnect Interval	Defines the time interval in seconds allowed for reconnection attempts to succeed. The valid range is between 1 and 5 seconds, with a default of 5 seconds.
Pause Attempts	Defines the time interval in minutes between reconnection attempts. The valid range is between 5 and 20 minutes, with a default of 20 minutes.

Stream Processor

The Stream Processor is an enhancement to the DSI Transporter Client, which enables streaming of GSX records directly to DSI. On the DSI, Stream Processor front ends the CDR data from up to 8 Transporter clients to a dedicated Transaction Processor for generating signaling analysis messages. The Stream Processor category allows you to **Create**, **Remove**, **Update**, and **Show** Stream Processor objects. The following table provides definitions of the various fields used in the **Create** and **Update** commands.

Stream Processor Create Field Definitions

Field	Definition
Name	The name of the Stream Processor (32 characters maximum) This field is read only on the Update interface
In Port	This field defines the IP port used by the Stream Processor frontend server to receive connection requests from the Transporter Clients. Valid entries must be between 5001 and 65535 with a default value of 15001.
Out Port	This field defines the IP port used by the Stream Processor frontend server to send CAM records to the dedicated TP for processing. Valid entries must be between 5001 and 65535.
BPA IP Address (optional)	The IP Address of the Business Partner Application receiving the records.
BPA Port (optional)	The Port of the Business Partner Application receiving the records. Valid entries must be between 5001 and 65535.
Filter Alive Records	Check to suppresses the ALIVE message. The default setting is unchecked.
Alive Frequency (optional)	This field defines the frequency that the Transporter Client generates the ALIVE message. This field is used by the Transporter Client only. Valid entries must be between 10 and 60 seconds with a default value of 30 seconds.
Reconnect Attempts (optional)	The number of times the Stream Processor should attempt to reestablish connectivity to the BPA system, if it loses connection. The valid range of values is between 1 and 60 with a default value of 5.
Attempt Interval (optional)	The amount of time in seconds that the Stream Processor should attempt to reestablish connection to the BPA system. The valid range of values is between 1 and 5 seconds with a default value of 5.
Pause Interval (optional)	The amount of time in minutes to wait between attempts to reestablish connection to the BPA system. The valid range of values is between 5 and 20 minutes with a default value of 5 minutes.
Active	The Stream Processor configuration entry will be recognized by the Stream Processor servers only if this flag is set. Default is unchecked.

Field	Definition
Out Configuration Name (optional)	Select the Output Connect object for association with this Stream Processor.
Max Records per File (optional)	Specifies the maximum number of billing records stored in a file. The default is 0, which signifies no limit set.
Max Size per file (optional)	Specifies the maximum size of a billing record file in kilobytes (KB). The default is 0, which signifies no limit set
Time Interval (optional)	Specifies the time interval for rolling over a billing record file. The default is 0, which signifies no limit set
SAI Stream	Flag to associate entries as either SAI or MATS. Checked = SAI; unchecked = MATS

DataStream Integrator Object

The Show command executes automatically, when you select the DataStream Integrator object from the tree. The show command displays the version information for the DSI, Adaptors, and Viewers. Also displayed is the Uptime (of the node) and an indicator of whether the DSI is suspended and if so, the reason for suspension.

There are three additional commands available from the Data Stream Integrator category:

DataStream Integrator Commands

Command	Definition
Reload Parameters	Used to activate changes made to the ConnectorDefinition, dsi_config, and Route Definition files on the DSI.
Stop DSI	Used to stop the DSI to implement changes requiring restarts (for example, the creation of new NFS Routes)
Start DSI	Used to start the DSI to after making changes requiring stops and restarts.

Alarm Manager

There are several types of DSI alarms that you must clear manually. The DSI Alarm Manager provides you the ability to clear these alarms. When you clear an alarm from the DSI using this interface, the system also sends a clearing trap to the Insight Fault Manager.

Through this interface you can also create test alarms by selecting the **Create Test Alarms** command and then selecting the **Type** (Critical, Major, or Minor).

To clear an alarm select the Clear Alarm command and then select the alarm Type from the list. The following table provides additional information concerning the alarm types.

DSI Alarm Manager Clearing Commands

Type	Definition
AlarmSetDiskFull AlarmSetDisk90 AlarmSetDisk75 AlarmSetDisk50	Allows you to clear alarms relating to disk space issues.
AlarmMinorCDRRecErr AlarmMajorCDRRecErr AlarmCDRFileReadErr AlarmCDRPartProc AlarmCDRNoOutput AlarmMinorCDRRecovery	Allows you to clear CDR related alarms (generated by CAM errors) of the designated type.
AlarmDDIErrorDM1 AlarmDDIErrorDM2 AlarmDDIErrorDM3 AlarmDDIErrorDM4	Allows you to clear all alarms (regardless of alarm level) raised for the designated Data Manager.
AlarmDDIErrorGeneric	Allows you to clear all alarms raised for generic DDI protocol errors.
AlarmSeqErr	Allows you to clear all of the alarms generated for missing CAM sequence numbers.
AlarmFilePullErr	Allows you to clear the File Pull alarm raised due to a failure to transfer AMA files.
AlarmIOReadErr AlarmIOWriteErr	Allows you to clear all alarms raised as a result of IO Read or Write Operations.
AlarmTesMajor AlarmTestMinor AlarmTestCritical	Allows you to clear a test alarm by level.
AlarmAMACreateErr	Allows you to clear all alarms raised as a result errors encountered during the creation of AMA files.

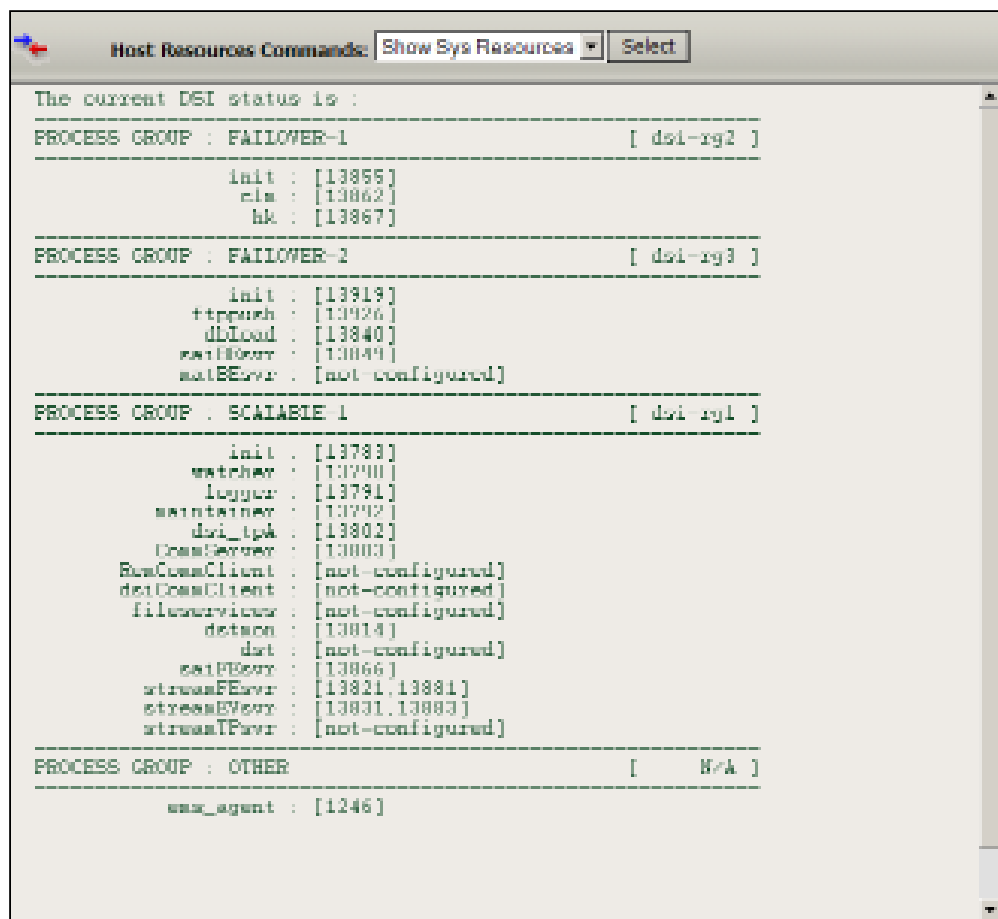
Type	Definition
AlarmFTPSessionFail AlarmFTTPersSesFail AlarmFTPFailAuthLoc AlarmFTPFailAuthRem	Allows you to clear alarms relating to either FTP session limits or authentication errors as specified.
AlarmFTPOutPriFilesMiss	Allows you to clear all alarms raised as a result of missing primary AMA files meant for transfer to DPMS.
AlarmStorageError	Allows you to clear all general Storage alarms.
AlarmStorageAllocFailure	Allows you to clear all of the Storage Allocation alarms generated due to missing sequence numbers.
AlarmStorageWriteFailure	Allows you to clear all of the Storage Write alarms generated due to missing sequence numbers.
AlarmStorageReadFailure	Allows you to clear all alarms indicating that the system was unable to access a file due to file permission problems or that the file did not exist.
AlarmSoftwareError	Allows you to clear all of the Software alarms generated due to missing sequence numbers.
AlarmFailoverEvent AlarmStartupEvent AlarmShutdownEvent	Allows you to clear alarms indicating either a Failover event, Startup Event, or a Shutdown event.
AlarmDSIFailure	Allows you to clear alarms indicating that an Mnode failed.
AlarmTelnetFailAuthRem	Allows you to clear all of the Telnet Authorization alarms.
AlarmSeqRestart	Allows you to clear alarms related to the loss of the current AMA file sequence number.
AlarmBECommDown AlarmBECommError	Allows you to clear errors indicating either that the Back End Stream Server is down or is experiencing communication problems.
AlarmFSProcessingFail AlarmFSSoftwareFail AlarmFSPeerCommFail AlarmFSFileSourceFail	Allows you to clear errors indicating problems with File Services software, communications, file manipulation, or processing.

Type	Definition
AlarmOpModeError	Allows you to clear errors indicating that a process cannot function under the current Operating Mode setting.
AlarmInPriFilesMiss	(No longer used) Allows you to clear errors indicating that indicates the DSI detected a missing AMA/CDR file not received from the GSX/PSX.
AlarmInterfaceDown	Allows you to clear errors indicating that the interface between the primary and secondary Mnodes in a Cluster is down.
AlarmEamaInitFailure	Allows you to clear an AlarmEamaInitFailure error.
AlarmDeviceError	Allows you to clear device errors detected by the HA monitor.

Host Resources

Selecting the Host Resources category from the object tree and then selecting the Show Sys Resources command displays information concerning the host system's Process Groups/processes as shown in the following figure.

Show System Resources Display



Log Manager

Additional articles:

- [Audit Trail](#)

The Log Manager category allows you to adjust the event messages recorded in the DSI daily log files by adding or removing event message categories (called log levels) from the list of events reported.

Clicking on the Log Manager category automatically displays the results of a Show command. From this interface you can set three parameters that control the generation and retention of log files.

Log Manager Show Field Definitions

Field	Definition
Max File Age	Specifies the number of days, between 1 and 14, that the system retains log files in the log directory. If the age of a log file exceeds the setting, the system automatically deletes it from the log directory. The default value is 3.

Field	Definition
Max File Size	Specifies the maximum file size (in bytes) for log files. When a log file reaches this limit, the logger automatically creates a new daily log file. The default setting is 5 MB (5,242,880 bytes).
NOTE: While the system will produce log files up to 2 GB in size, most text editors will not open a file this large.	
Max Logs per Day	Specifies the maximum number of logs produced each day. This is in addition to the log currently open. For example, if Max Logs per Day = 3 , then the maximum number of logs with today's date that exists in the DataStream Integrator log directory is 4, 3 plus 1 currently open. The setting must be between 1 and 365. The default is 365.
Enable System Auditing	Check to enable auditing.

You add or remove a log level by selecting either the **Add Level** or **Remove Level** command from the Log Manager Command list and then selecting the four character code that denotes the type of event recorded. The following table a list of available log level codes.

Log Level Codes

Code	Definition
APPE	Application Error Log messages at this level indicate that an error occurred during the performance of some higherlevel system function. Many of the errors at this level indicate problems with normal system processing, such as problems linking to DLLs or problems loading the shared buffer file.
APPT	Application Trace Log messages at this level are a normal part of system functioning, such as session start or shutdown.
APPW	Application Warning Indicates that an application problem occurred, but that the error did not hinder system processing.
AUDE	Audit Error
AUDT	Audit Trace
AUDW	Audit Warning
DB_E	Database Error Log messages at this level indicate that an error occurred during the execution of a database command. Because this error indicates a problem with the DSI accessing the necessary database information, it requires immediate attention.

Code	Definition
DB_T	Database Trace Log messages at this level are informational and used to assist in tracking the condition of the database.
DB_W	Database Warning Log messages at this level indicate that a relatively minor error occurred during the execution of a database command and that the system either localized, or handled the error.
INFP	Code for normal log entries during DataStream Integrator operations.
INFT	Code for detailed log entries during DataStream Integrator trace operations.
MI_E	Adaptor Error This indicates an error occurred in the Generic Message Interface subsystem of the DSI. Because this error indicates that the DSI cannot perform a necessary key processing task, it requires immediate attention.
MI_T	Adaptor Trace Log messages at this level are informational and used to assist in tracking the progress of a job in the Generic Message Interface subsystem of the DSI.
MI_W	Adaptor Warning, This indicates a relatively minor error occurred in the Generic Message Interface subsystem of the DSI and that the system either localized, or handled the error.
SYSE	Host System Error May indicate a serious problem with the underlying operating system. Many of the errors at this level are beyond the control of the application, such as permission problems, low memory, or low disk space.
SYST	Host System Trace Log messages at this level are informational and used to assist in tracking the results of system calls.
SYSW	Host System Warning indicates that a problem existed in the operating system. The application attempts to compensate for these problems, but the presence of these log messages indicates that future problems could occur.

To display the current Log levels, select the **Show Log Levels** command from the Log Manager command list.

You can also search the log files for particular entries. To search the log files, select **Find in Logs** from the Log Manager command list, enter a string into the **searchVal** field and **Submit**. The system searches all listed log files for the string and displays the results.

Note

If the size of your search results exceed 64 kilobytes of information, the system returns an error message. If this occurs, you must narrow your search.

You can view the contents of individual Log Files by selecting the file (checking the Select check box next to the file name) and executing the **Show** command. The contents of the selected Log File display in a new viewing window.

For additional information concerning the DSI log files and their format, refer to the [Administering and Maintaining DSI](#) documentation.

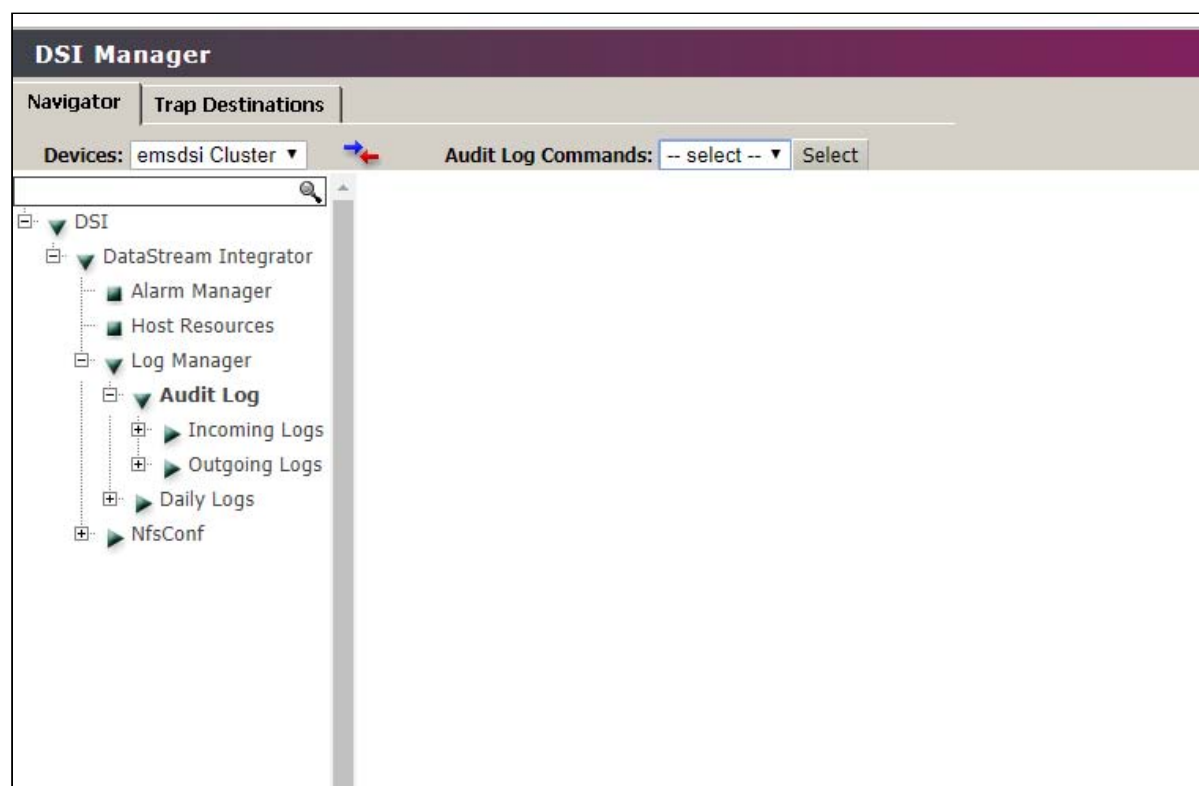
Audit Trail

The DSI provides an audit log facility that can be used to account the disposition of files and records processed by DSI against those files received. The transfer of files between DSI and any 3rd Party Servers may happen to have incidental transactional information logged to the DSI application log file. However, as a formal record supporting audit and confirmation of transfers between DSI and a 3rd Party server, minimally complete record information is not logged as a matter of course. Moreover, such audit details need to be captured in a dedicated log structure (separate from the DSI daily log file) for the exclusive purpose of auditing devoid of unrelated information and subject to specialized retention configuration settings.

These details are captured in the “Audit Logs” which further contain two logs for each node, Incoming and Outgoing. Each node has an incoming and outgoing log for each destination entry.

The Audit Logs contain two logs for each node, Incoming and Outgoing. Each node has an incoming and outgoing log for each destination entry.

Audit trail



NFS Configuration

Additional articles:

- [Create NFS Client](#)

DSI acts as NFS server for the Ribbon network elements. Using the DSI Manager, NFS configuration can be restricted to the intended clients based on their IP address or netmask. The clients can be created, updated, viewed or deleted.

To view the NFS client, select **Show** from the Command drop-down menu. The configured NFS client and the respective directories mounted on the share appear.

To delete the NFS Client, select Delete from the Command drop-down menu. Then, select the hostnames to delete.

Deleting hostname deletes the hostname entries and all the associated IP addresses of the host from NFS configuration. For deleting a particular IP Address, update the existing Host Name and delete the particular IP Address such that the IP Address field is blank.

Create NFS Client

NFS client can be configured based on hostname, IP address, and directory structure. The directory access is limited to `/export/home/SonusNFS` or `/global/home/SonusNFS`.

Note

Before creating a configuration on a particular directory, check if the directory is created on that DSI.

To configure NFS client, select Create from the command drop-down menu. Then, provide the hostname, directory server, and IP address. The table below details the parameter list for the Create command:

Parameter list for Create command

Field	Description
hostname	Defines the NFS client hostname.
directory	Specifies if the directory structure is /export/home/SonusNFS or /global/home/SonusNFS.
IPAddr1	Specifies the first restricted client's IP Address.
IPAddr2	Specifies the second restricted client's IP Address.
IPAddr3	Specifies the third restricted client's IP Address.
IPAddr4	Specifies the fourth restricted client's IP Address.
IPAddr5	Specifies the fifth restricted client's IP Address.
IPAddr6	Specifies the sixth restricted client's IP Address.
IPAddr7	Specifies the seventh restricted client's IP Address.
IPAddr8	Specifies the eighth restricted client's IP Address.

Note

While updating the existing entry, only the IPAddr1 to IPAddr8 can be updated and hostname or directory cannot be updated. This is done to support single IP deletion from CLI.

Trap Destinations

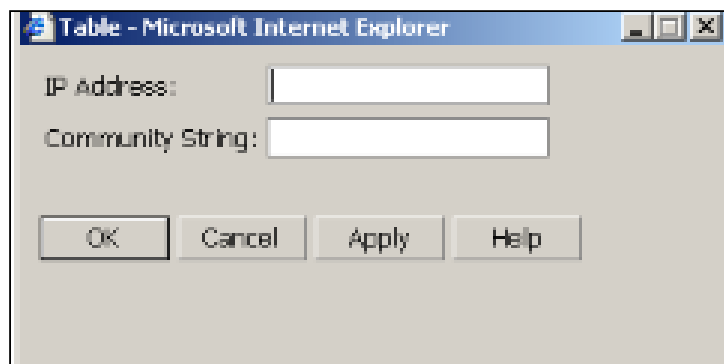
The Trap Destination tab of the DSI Manager window allows you to add or delete trap destinations for selected, registered DSI nodes.

Trap Destination GUI

DSI Manager		
Navigator	Trap Destinations	
Node: Dsi	Add	Remove
Select	Trap Destination	Community
☐	10.54.49.103	*****
☐	10.54.49.101	*****
☐	10.34.146.9	*****
☐	10.54.48.96	*****
☐	10.54.13.236	*****
☐	10.54.48.138	*****
☐	10.54.53.00	*****

To add a destination, first select a registered node from the Node list box. Click the **Add** button to open the Add Destination dialog box. Enter the **IP Address** and the **Community String** of the destination node. Click **OK** to add the destination to the table and close the dialog box, or click **Apply** to add this destination and keep the dialog box open.

Add Trap Destination GUI



To delete a destination from the table, check the box next to the entry you wish to delete and click the **Remove** button. Click **OK** in the confirmation dialog box.

Launch Edge 8000 GUI

Launch an Edge 8000 GUI from Ribbon Application Management Platform (RAMP) as described below.

Prerequisites

- The Edge 8000 is registered on RAMP.
- RAMP Super User privileges for the **Insight Administration** resource under the **Core Resources** application. Refer to [User Privileges in RAMP](#).
- RAMP **Devices** and **Resource Groups** privileges under the **Device Management** application. Refer to [User Privileges in RAMP](#).

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list, in the row for the Edge 8000 device you want to configure, click on the ellipses (...) menu and select **Configure**. RAMP launches the Edge 8000 GUI for the device.

For more information on configuring Edge 8000 devices, refer to [Edge 8000 Documentation](#).

Launch EdgeMarc GUI

Launch the EdgeMarc GUI from the Ribbon Application Management Platform (RAMP) to configure EdgeMarc devices.

Prerequisites

- The EdgeMarc device is registered on RAMP.
- Possess Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- Possess **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. Select the EdgeMarc device to configure.
4. In the nodes list, in the row for the EdgeMarc device to configure, click on the ellipses (...) menu and select **Configure**.
5. Log on to the EdgeMarc GUI.

Launch G5 GUI

Launch the G5 Line Access Gateway devices (G5) GUI from Ribbon Application Management Platform (RAMP) to configure G5 devices.

Prerequisites

- The G5 device is registered on RAMP.
- You must have Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list, in the row for the G5 device you want to configure, click on the ellipses (...) menu and select **Configure**. The G5 window opens.
4. Log into the GUI using your login credentials.

For more information refer to, [G5 Line Access Gateway Documentation](#).

Launch G6MM GUI

Launch the G6MM GUI from Ribbon Application Management Platform (RAMP) to configure G6MM devices.

Prerequisites

- The G6MM device is registered on RAMP.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list, in the row for the G6MM device you want to configure, click on the ellipses (...) menu and select **Configure**. The G6MM window opens.
4. Log into the GUI using your login credentials.

For more information on configuring G6MM devices, refer to [G6 Universal Gateway Documentation](#).

Launch GMS GUI

Launch the GMS GUI from Ribbon Application Management Platform (RAMP) to configure GMS devices.

Prerequisites

- The GMS device is registered on RAMP.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list, in the row for the GMS device you want to configure, click on the ellipses (...) menu and select **Configure**. The GMS window opens.
4. Log into the GUI using your login credentials.

For more information on configuring GMS devices, refer to [General Media Server Documentation](#).

Launch GSX GUI

In this section:

- [Launching GSX Navigator from RAMP](#)
- [Working with GSX Navigator](#)
 - [Node Discovery and Status](#)
 - [Live Software Upgrade Status](#)
 - [Initiate a Command on an Object](#)
 - [Commands for an Entire Trunk Group](#)
- [GSX Navigator Procedures](#)
 - [Configure Local Redirection Attempt Records](#)
 - [Configure SIP Service Group](#)
 - [Configure ISUP Services](#)
 - [Configure ISUP Service Profiles](#)

Related articles:

- [Scheduling Report Data Collection](#)
- [Creating Reports Using GSX Navigator](#)
- [Event Log](#)
- [Verifying the Database Status](#)
- [Configuring GSX Call Trace Filters](#)

- [Create CPC to ISUP Cause Mapping Profiles](#)
- [Configure CPC to ISUP Cause Mapping](#)
- [Configure CPC to SIP Cause Mapping](#)
- [Configure SIP to CPC Cause Mapping](#)

The GSX Navigator is a Graphical User Interface (GUI) used to issue CLI commands to a GSX Open Services Switch. The GSX Navigator provides visibility to all managed objects within a GSX device (GSX9000) and access to the commands associated with each object. **Ribbon Application Management Platform (RAMP)** automatically discovers all supported objects on GSXs registered with it. When an object requires configuration, you can select it from the object tree, select the desired command from the Commands list, and then provide any additional parameters that are required in the windows provided.

For detailed information on the operation of the commands available from **GSX Navigator**, see [GSX9000 Operations and CLI Reference](#).

Note

The Show IPv6 NetStat All TCP Connection Status command is not available in GSX Navigator. The command can be entered only through GSX CLI.

You can use the GSX Navigator to configure call tracing filters and then view the output on **RAMP**. Refer to [Call Trace](#).

For a limited number of objects, you can also use **GSX Navigator** as a launching point for real-time and historical performance charts. Refer to [Creating Reports Using GSX Navigator](#).

You can configure the maximum number of GSX Navigator windows that can be opened simultaneously. For more information, refer to [Configure Device Management Administration Options](#).

Launching GSX Navigator from RAMP

Use the following procedure to launch the GSX Navigator.

Prerequisites

- The GSX device is registered on **RAMP**.
- The GSX device is up and running.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- Super User [privileges](#) for **Configuration Management** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the **RAMP** GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the row for the GSX device you want to work with, click on the ellipses (...) menu and select **Configure**. The **GSX Navigator** window opens.

Working with GSX Navigator

The following sections provide information on working with GSX Navigator.

Node Discovery and Status

RAMP synchronizes with registered GSX nodes detecting the latest information for all the objects contained on each. When different RAMP or CLI users create and modify objects, the Object tree updates to reflect those changes. Typically, this happens automatically. The status field at the bottom left the object tree displays the state of the tree.

The system displays one of five states for the selected GSX with respect to discovery and reachability.

- **Up To Date** — The GSX object tree has the most current data for the selected node. The background color of the status field is grey.
- **Out Of Date** — The tree is not up to date. Click the Discover button to initiate a discovery manually updating the tree with the latest data. The background color of the status field is orange.
- **Discovering** — The tree is in the process of updating. The background color of the status field is green.
- **Error** — An error occurred during discovery. The background color of the status field is red.
- **Unreachable** — The GSX node is not responding to SNMP requests. The background color of the status field is red.

Live Software Upgrade Status

The field at the bottom right of the GSX Navigator object tree displays the current software version of the GSX software. The field indicates one of four states with respect to the software version.

- **Normal** — The software version number displays in normal type and the background color of the software version field is grey.
- **Software Update In Progress** — The software version number displays in italics and the background color of the software version field is orange. While in this state, the system disables the discovery button, most CLI operations, and Performance Monitoring.
- **Software Update Failure** — The software version number displays in italics with a question mark (?) appended. The background color of the software version field is red. In this state, the system requires operator action either to complete the software update successfully, or to halt the software update.
- **Commit Pending** — The software version number displays in italics with a plus sign (+) appended. The background color of the software version field is green. In this state, the system requires operator action to commit the software update.

Initiate a Command on an Object

To initiate a command once the GSX Navigator is open:

1. Select a node from the **Devices** list. This list displays all GSX nodes registered with RAMP and belonging to Resource Groups associated with the user (see [User Privileges in RAMP](#)).
The Objects tree displays all of the managed objects for the selected GSX node. The tree may take several seconds to load.
2. Select an object from the object tree. To show objects contained within folders, expand the folders by clicking on the + sign.
The Command list reflects all commands available for the selected object.
3. Choose a command from the Command list. The command executes automatically upon selection. Click **Select** to refresh the active command.
If the selected commands does not require additional user input, the results display directly in the work space area. If the selected command requires additional user input, a Command window appears, allowing you to input the required parameters.

Note

Only users with Provisioner or Super User privileges have access to the Create, Delete and Configure commands. Also, administrators can limit user access on a individual command basis. Refer to [Restrict Access to GSX Commands](#).

Note

When the GSX Navigator invokes Task Configurator scripts to execute tasks, the “Stop if element exists” parameter is always set to “True.” This setting checks for existing GSX entries with the specified name (such as inservice Trunk Groups) and prevents them from being overwritten when new objects are provisioned on the node

4. Enter/select the parameters in the Command window as necessary.
5. Click **OK** to issue the command. Error messages and outputs for the commands display in the work space area.
6. To automatically update the output of a Show command at a selected interval use the **Redo** command, selecting an “interval” x “number of times” setting from the list. The Redo icon animates while initiating the sequence. Upon completion of the sequence, the Redo selection returns to an inactive state. The system returns an error, if you attempt to use the Redo option on commands other than show.
7. You can terminate the Redo command at any time, by either selecting another command that does not require additional input (If the new command requires additional input, the Redo command remains active until you complete and execute the new command), or by manually setting it to inactive.

Commands for an Entire Trunk Group

There are commands available from the GSX Navigator that perform operations on an entire Trunk Group hierarchy. None of the following operations require any input parameters, as **RAMP** uses the configuration information retrieved from the GSX to determine the trunk group hierarchy. For these operations to be successful, you must ensure that PIF collection is up-to-date for the selected GSX(s).

Caution

Each of the following commands are service affecting.

Command	Description
Bounce BT IUP Trunk Group Hierarchy	This command sets the Trunk Group hierarchy to a disabled state and then reenables it. Since objects in the hierarchy are put into outOfService mode using the action FORCE, this operation will disrupt existing calls. You should use this command only if the Trunk Group hierarchy has been frozen into an unresponsive, nonoperating state.

Command	Description
Bounce CAS Trunk Group Hierarchy	This command sets the Trunk Group hierarchy to a disabled state and then re-enables it. Since objects in the hierarchy are put into outOfService mode using the action FORCE, this operation will disrupt existing calls. You should use this command only if the Trunk Group hierarchy has been frozen into an unresponsive, nonoperating state.
Bounce ISDN NFAS Trunk Group Hierarchy	This command sets the ISDN NFAS Trunk Group hierarchy to a disabled state and then re-enables it. Since objects in the hierarchy are put into outOfService mode using the action FORCE, this operation will disrupt existing calls. You should use this command only if the Trunk Group hierarchy has been frozen into an unresponsive, nonoperating state.
Bounce ISDN PRI Trunk Group Hierarchy	This command sets the ISDN PRI Trunk Group hierarchy to a disabled state and then reenables it. Since objects in the hierarchy are put into outOfService mode using the action FORCE, this operation will disrupt existing calls. You should use this command only if the Trunk Group hierarchy has been frozen into an unresponsive, nonoperating state.
Bounce ISUP Trunk Group Hierarchy	This command sets the Trunk Group hierarchy to a disabled state and then reenables it. Since objects in the hierarchy are put into outOfService mode using the action FORCE, this operation will disrupt existing calls. You should use this command only if the Trunk Group hierarchy has been frozen into an unresponsive, nonoperating state.
Delete BT IUP Trunk Group Hierarchy	This command deletes the following objects in this order: the BT IUP Circuits contained in the Trunk Group hierarchy, the BT IUP Services contained in the hierarchy, and the selected Trunk Group. You can use this command to delete unused trunk groups and contained objects in a single operation.
Delete CAS Trunk Group Hierarchy	This command deletes the following objects in this order: the CAS Circuits contained in the Trunk Group hierarchy, the CAS Services contained in the hierarchy, and the selected Trunk Group. You can use this command to delete unused trunk groups and contained objects in a single operation.
Delete ISDN NFAS Trunk Group Hierarchy	This command first disables the selected Trunk Group and its contained ISDN Interfaces and BChannels and then deletes it. You can use this command to delete unused trunk groups and contained objects in a single operation.

Command	Description
Delete ISDN PRI Trunk Group Hierarchy	This command first disables the selected Trunk Group and its contained ISDN Interface and BChannels and then deletes it. You can use this command to delete unused trunk groups and contained objects in a single operation.
Delete ISUP Trunk Group Hierarchy	This command deletes the following objects in this order: the ISUP Circuits contained in the Trunk Group hierarchy, the ISUP Services contained in the hierarchy, and the selected Trunk Group. You can use this command to delete unused trunk groups and contained objects in a single operation.
Disable BT IUP Trunk Group Hierarchy	This command disables the following objects in this order: the BT IUP Circuits contained in the Trunk Group hierarchy, the BT IUP Services contained in the hierarchy, and the selected Trunk Group.
Disable CAS Trunk Group Hierarchy	This command disables the following objects in this order: the CAS Circuits contained in the Trunk Group hierarchy, the CAS Services contained in the hierarchy, and the selected Trunk Group.
Disable ISDN NFAS Trunk Group Hierarchy	This command disables the selected Trunk Group and its contained ISDN NFAS Trunks
Disable ISDN PRI Trunk Group Hierarchy	This command disables the selected Trunk Group and its contained ISDN PRI Trunks.
Disable ISUP Trunk Group Hierarchy	This command disables the following objects in this order: the ISUP Circuits contained in the Trunk Group hierarchy, the ISUP Services contained in the hierarchy, and the selected Trunk Group.
Enable BT IUP Trunk Group Hierarchy	This command enables the following objects in this order: the BT IUP Circuits contained in the Trunk Group hierarchy, the BT IUP Services contained in the hierarchy, and the selected Trunk Group.
Enable CAS Trunk Group Hierarchy	This command enables the following objects in this order: the CAS Circuits contained in the Trunk Group hierarchy, the CAS Services contained in the hierarchy, and the selected Trunk Group.
Enable ISDN NFAS Trunk Group Hierarchy	This command enables the selected Trunk Group and its contained ISDN NFAS Trunks.
Enable ISDN PRI Trunk Group Hierarchy	This command enables the selected Trunk Group and its contained ISDN PRI Trunks.

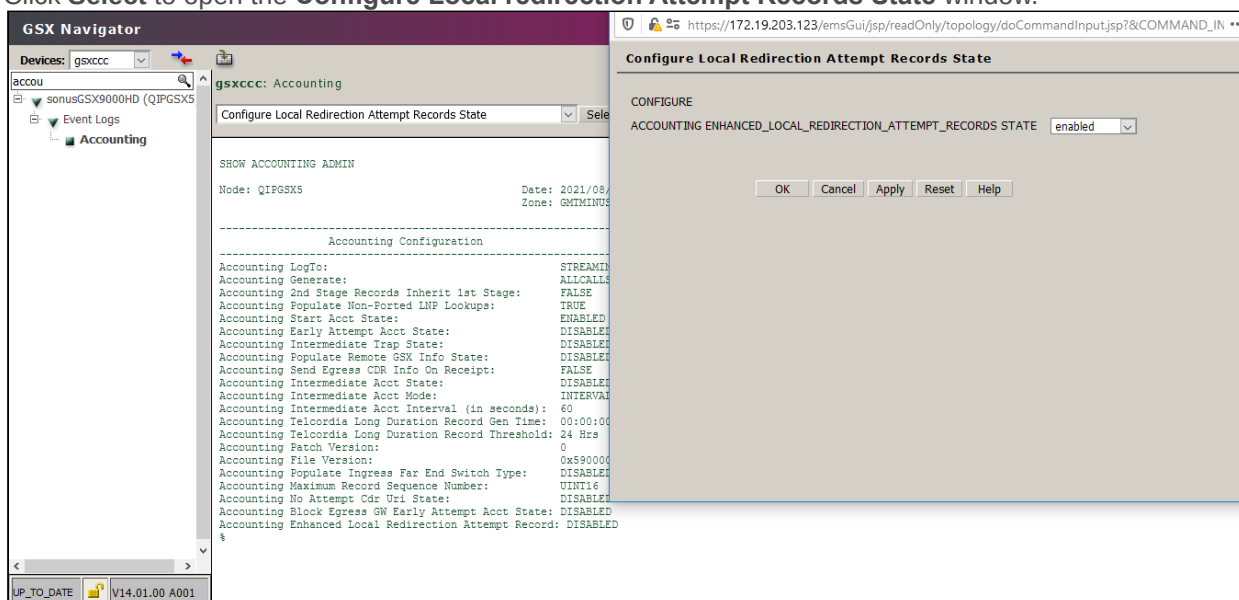
Command	Description
Enable ISUP Trunk Group Hierarchy	This command enables the following objects in this order: the ISUP Circuits contained in the Trunk Group hierarchy, the ISUP Services contained in the hierarchy, and the selected Trunk Group.

GSX Navigator Procedures

The following sections describe tasks that can be completed after you launch GSX Navigator for a selected GSX node.

Configure Local Redirection Attempt Records

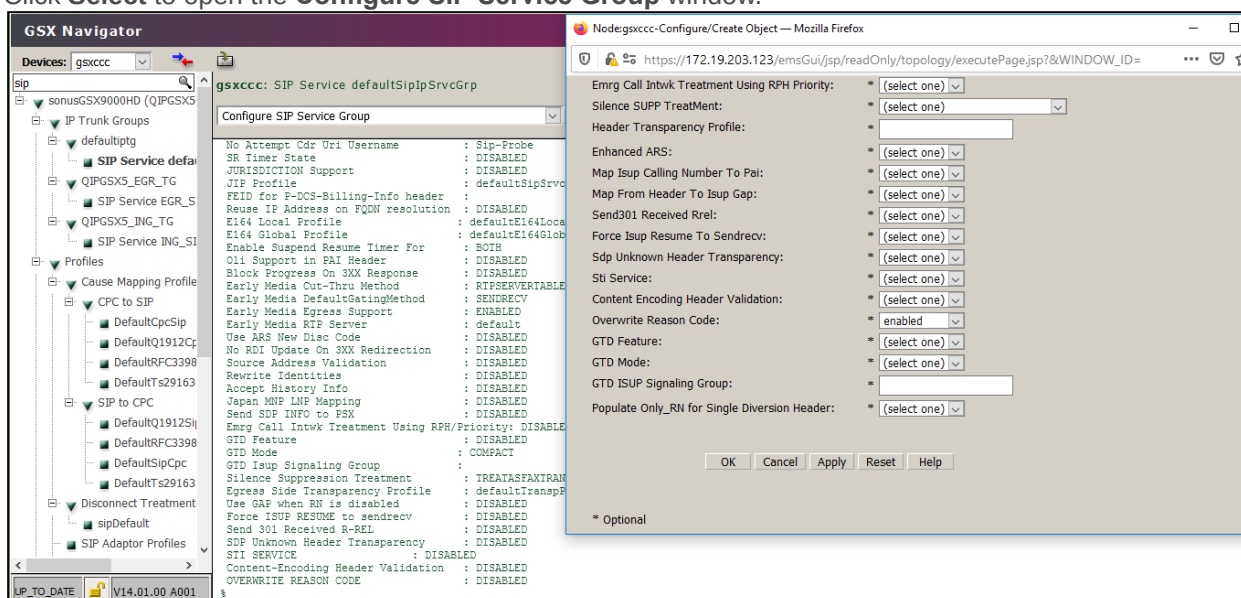
1. Click **Accounting**.
2. Select **Configure Local redirection Attempt Records State** from the drop-down list.
3. Click **Select** to open the **Configure Local redirection Attempt Records State** window.



Configure SIP Service Group

1. Click **Configure SIP Service defaultSipIpSrvGrp**.
2. Select **Configure SIP Service Group** from the drop-down list.

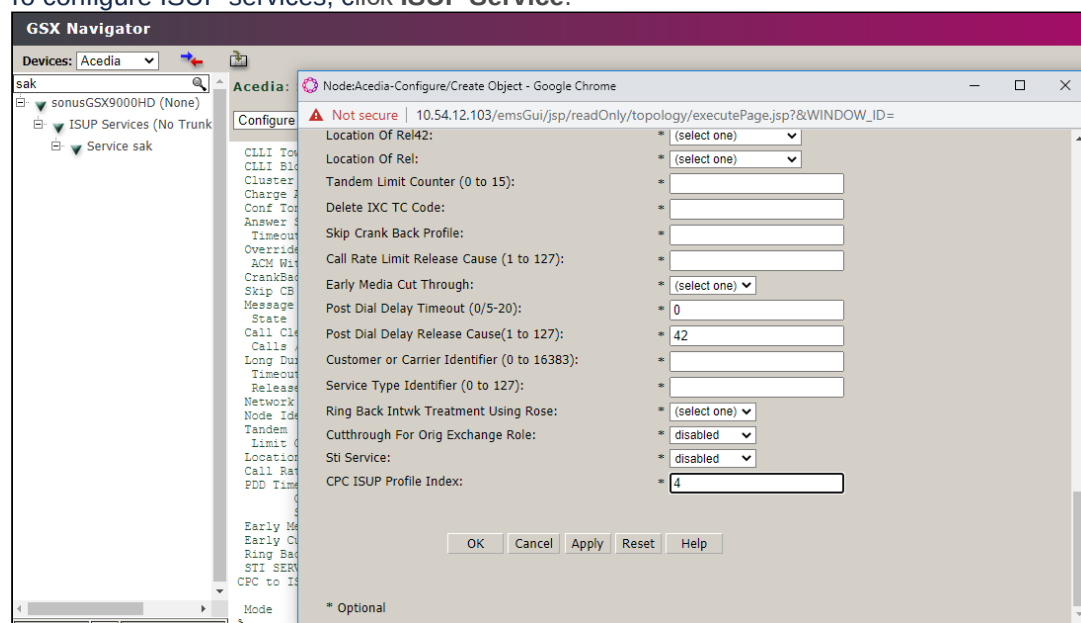
3. Click **Select** to open the **Configure SIP Service Group** window.



4. Select **enable** or **disable** for the options as appropriate.
5. Click **OK**.

Configure ISUP Services

To configure ISUP services, click **ISUP Service**.

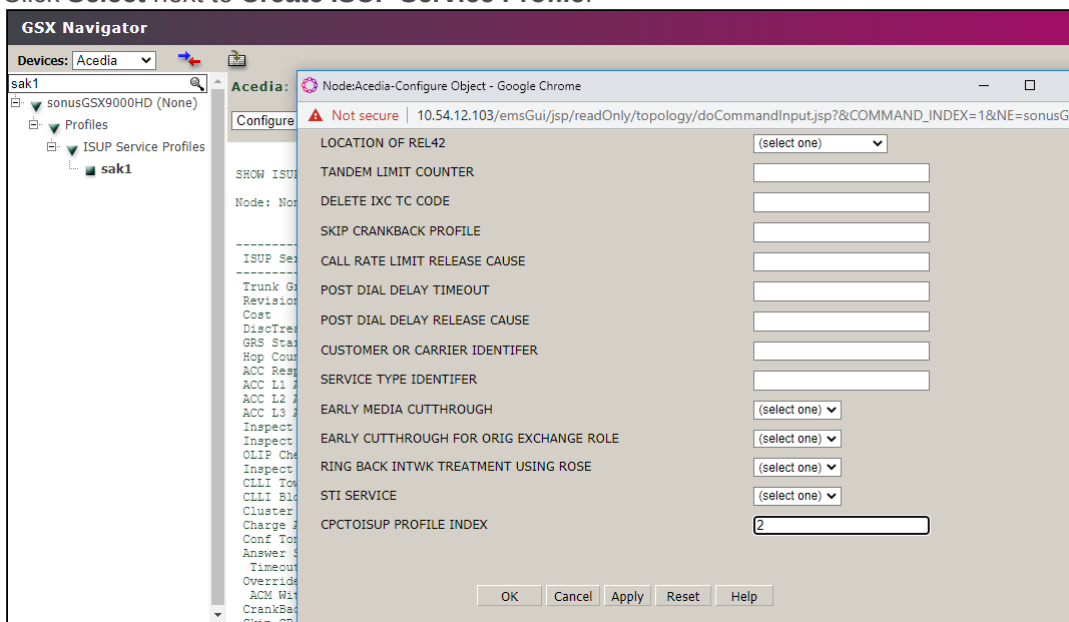


Configure ISUP Service Profiles

To configure an ISUP Service Profile:

1. Navigate to **Profiles > ISUP Service Profiles**.
2. Click on **ISUP Services Profiles**.

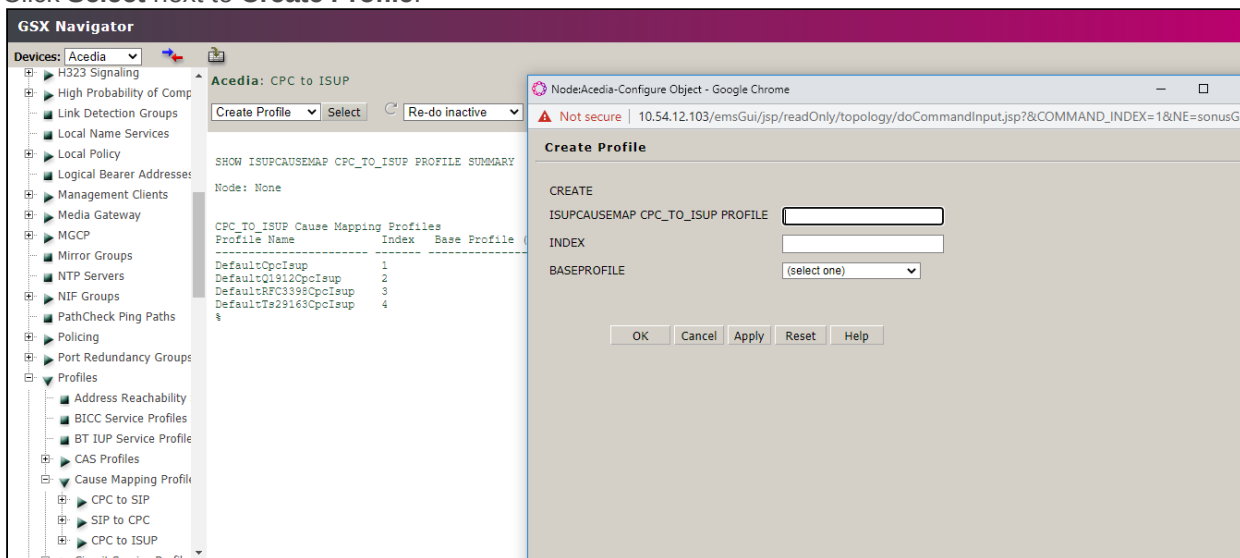
3. Click **Select** next to **Create ISUP Service Profile**.



Create CPC to ISUP Cause Mapping Profiles

To create a CPC to ISUP cause mapping profile:

1. Navigate to **Profiles > Cause Mapping Profiles > CPC to ISUP**.
2. Click **Select** next to **Create Profile**.

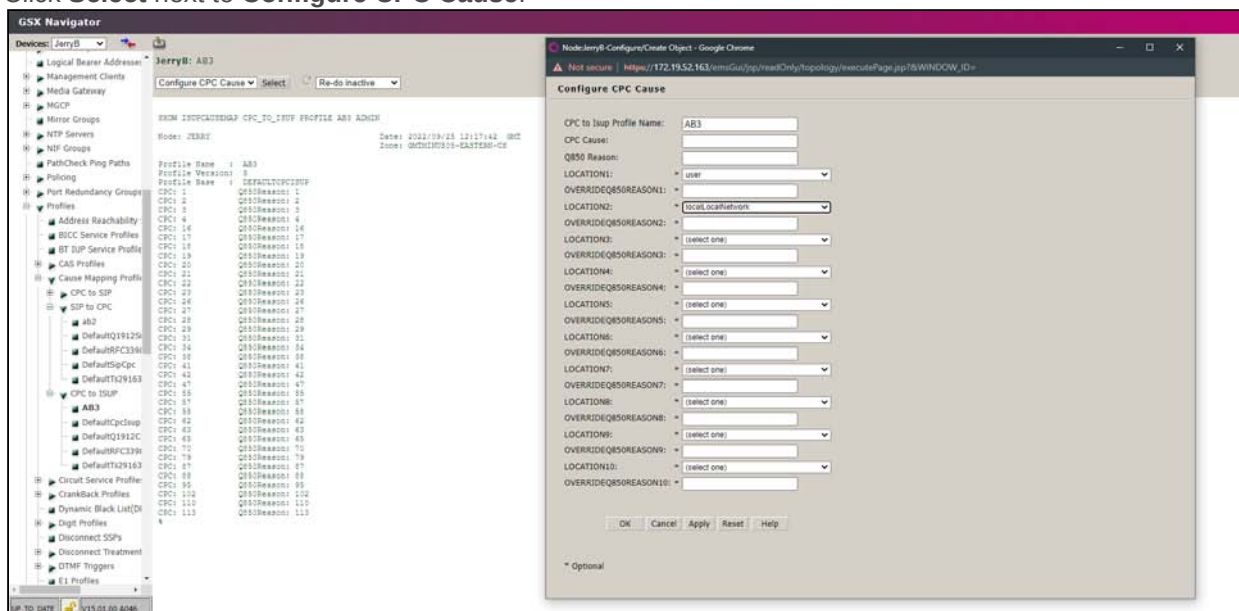


Configure CPC to ISUP Cause Mapping

To configure CPC to ISUP cause mapping:

1. Navigate to **Profiles > Cause Mapping Profiles > CPC to ISUP**.
2. Select a profile to configure.

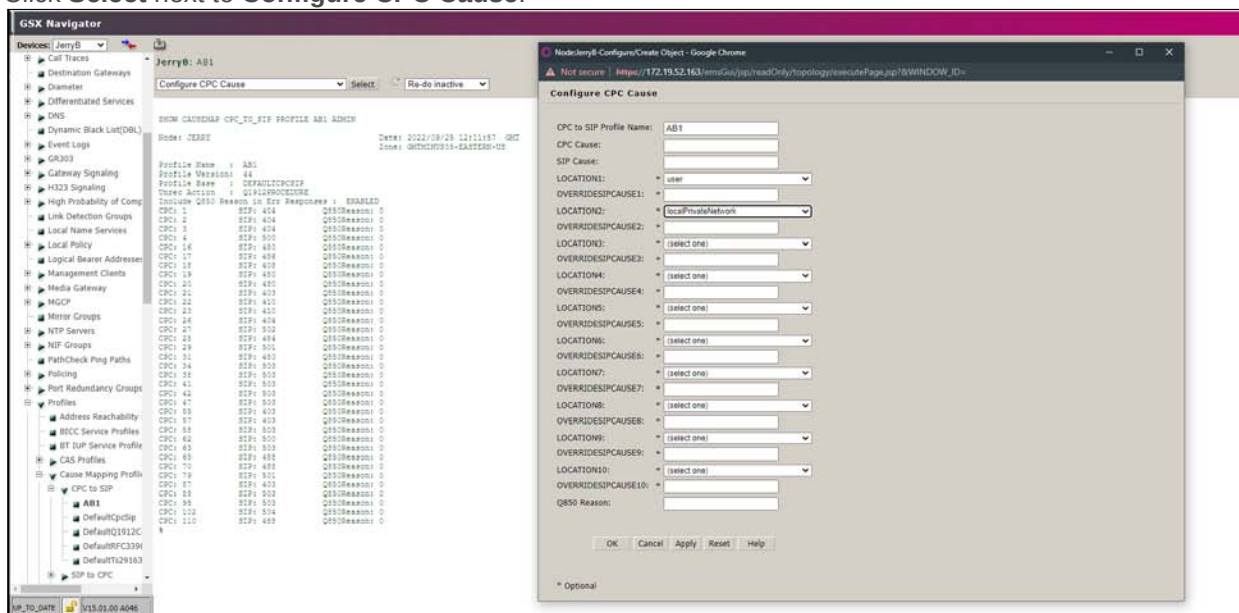
3. Click **Select** next to **Configure CPC Cause**.



Configure CPC to SIP Cause Mapping

To configure CPC to SIP cause mapping:

1. Navigate to **Profiles > Cause Mapping Profiles > CPC to SIP**.
2. Select a profile to configure.
3. Click **Select** next to **Configure CPC Cause**.

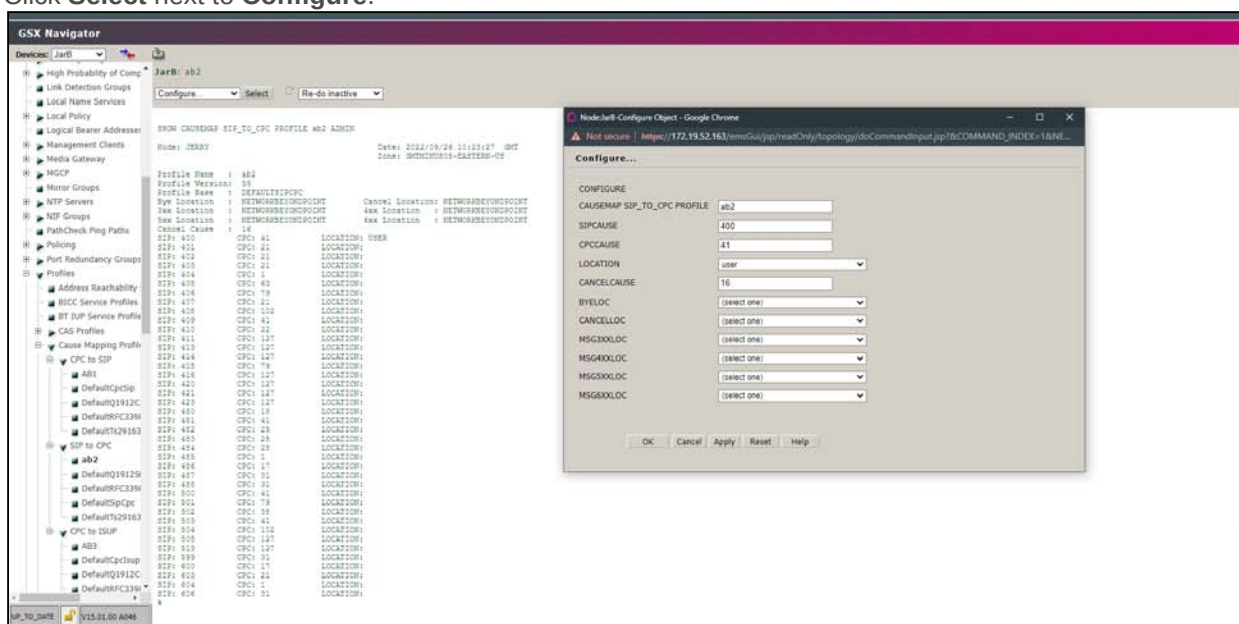


Configure SIP to CPC Cause Mapping

To configure SIP to CPC cause mapping:

1. Navigate to **Profiles > Cause Mapping Profiles > SIP to CPC**.
2. Select a profile.

3. Click **Select** next to **Configure**.



Scheduling Report Data Collection

On Ribbon Application Management Platform (RAMP) you can enable the acquisition of configuration data in the form of Parameter Interchange Format (PIF) files from GSXs. Through the settings in the **Report Data Collection** window, you can submit a request to collect configuration data from a GSX immediately, schedule the collection on a node-by-node basis, set the system wide collection parameters, and verify the current status of the configuration data in the RAMP database.

You can also enable the use of incremental PIFs as a less resource intensive method of updating the report information. An incremental PIF is a file representing only the configuration information that has changed since the last full PIF file retrieval and is therefore considerably smaller than the full PIF file.

Depending upon the number of DS0s and trunk groups configured on the GSX, network latency, and the RAMP server processing load, the total time required to collect and store the configuration data in the RAMP database can exceed 10 minutes per node.

Prerequisites

- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- Super User [privileges](#) for **Configuration Management** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.
- A GSX node is registered on RAMP.
- The GSX device is up and running.
- Data collection is enabled for the GSX node on RAMP.
- A trunk group is configured on the GSX.

Procedure

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the row for the GSX device you want to work with, click on the ellipses (...) menu and select **Configure**. The **GSX Navigator** window opens.
4. Click the "Report data collection" icon in Toolbar to open the **Report Data Collection** window.
5. Select the **Collection** tab to display the Collection options.
6. Set the **Collection Enabled** field to **Yes**.

7. Use the **Synchronize on Insight Startup** field to enable/disable **RAMP** synchronization with registered GSXs for which you have previously enabled incremental pif data collection upon a **RAMP** reboot. If enabled, upon reboot, **RAMP** determines if new pif data collection, either incremental or full, is required to resynchronize the **RAMP** database with the actual GSX state. (default setting is No)
8. In the **File Collection Timeout** field, enter the number of seconds **RAMP** waits before determining that it cannot retrieve the GSX parameter file from the NFS mount point. (Default 300 seconds)
9. If you want to schedule daily file retrieval for a particular registered node, select the node by checking **Scheduled Enabled**, and set the desired time of day for configuration parameter file retrieval.

Note

The desired time of day for configuration parameter file retrieval may differ significantly from the actual time of retrieval and processing. The actual timing depends upon how many nodes you scheduled for collection, how many threads you configured for each activity, and the amount of time required for the processing of information from each node. If you schedule data collection for multiple GSXs, Ribbon recommends that you stagger the collection times to reduce the possibility of system resource overload.

10. If you want to enable the retrieval of incremental PIFs, select **Incremental Enabled** and set **Number of Collections** to the number of incremental PIFs you want the GSX to maintain on its primary and secondary mount points. (default = 1, max = 10)

Note

Ribbon recommends checking **Incremental Enabled** after you fully populate the GSX.

11. Click **Apply** to accept the configuration.

Creating Reports Using GSX Navigator

You can generate historical performance graphs and charts for GSX objects through the GSX Navigator.

GSX Objects with Performance Charts

Node Object	Report
Device	• Monitor Average Call Duration • Monitor Busy Hour Attempts • Monitor Call Attempt Rate • Monitor Call Failures • Monitor Call Attempts/Blocked • Monitor Call Attempts/Completions

Node Object	Report
Trunk Groups	• Monitor Call Setup Time • Monitor Inbound Attempts • Monitor Inbound BHA • Monitor Incoming Call Failures • Monitor Outbound Attempts • Monitor Outbound BHA • Monitor Outgoing Call Failures • Monitor Routing Attempts/Failures • Monitor Usage • Monitor Utilization Percent
All Slots	• Monitor CPU Utilization
CNS	• Monitor Active Calls • Monitor Call Attempt History
PNS10 Port	• Monitor Active Calls • Monitor Bandwidth Utilization
PNS20 Port	• Monitor Active Calls • Monitor Bandwidth Utilization
SoftSwitch	• Monitor SoftSwitch Average Transaction Time • Monitor SoftSwitch Connection Attempts • Monitor SoftSwitch Transaction
Destination Gateways	• Monitor Active Calls Between Gateways • Monitor BHA Between Gateways • Monitor Call Rate Between Gateways

Prerequisites

- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- Super User [privileges](#) for **Configuration Management** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.
- A GSX node is registered on RAMP.
- The GSX device is up and running.
- Data collection is enabled for the GSX node on RAMP.
- A trunk group is configured on the GSX.

Procedure

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window opens.
3. In the row for the GSX device you want to work with, click on the ellipses (...) menu and select **Configure**. The **GSX Navigator** window opens.
4. Select a node from the **Devices** drop-down list.

The Node Objects tree displays all managed objects for the selected GSX node. The tree may take several seconds to load.

5. Select an object from the tree that has performance measures.
6. Expand object folders to show objects contained within.
7. From the Command drop-down list, select a Monitor command.

The screenshot shows the GSX Navigator interface. On the left, a tree view lists various objects under the 'ACADIA' device. The 'TestIPTG' object is selected. A context menu is open over 'TestIPTG', showing a list of commands. 'Monitor Call Setup Time' is highlighted. To the right of the menu, a table displays the configuration for the selected command.

Command	Value
Monitor Call Setup Time	ENABLED
Monitor Inbound Attempts	0
Monitor Inbound BHA	INSERVICE
Monitor Incoming Call Failures	DRYUP
Monitor Outbound Attempts	5
Monitor Outbound BHA	NONE
Monitor Outgoing Call Failures	NONE
Monitor Routing Attempts/Failures	DISABLED
Monitor Usage	1
Monitor Utilization Percentage	1
Show Admin	10
Show All MLPP Status	DISABLED
SILC Congestion Level 2 Calls Allowed (percent)	075
Trunk Group Type	025
IP Trunk Group Direction	IPLINKED
Parent IP Trunk Group	BOTHWAYS
IP Network Selection Table	
IP Call Limit	UNLMT
IP Bandwidth Limit	UNLMT
Packet Outage Detection Minimum Duration	6000
Packet Outage Detection Minimum Calls	1000
Packet Outage Detection Bandwidth Limit Reduct	50
Packet Outage Detection State	DISABLED
Packet Outage Detection Interval (minutes)	15
Master Trunk Group Name	
Calls Requested Per MTRG Request	100
Bandwidth Requested Per MTRG Request (1K bps)	12400
Maximum Ingress Sustained Call Rate	0
Maximum Ingress Call Burst Size	0
Maximum Ingress Sustained SIP nonInvite Rate	0
Maximum Ingress SIP nonInvite Burst Size	0
Maximum Egress Sustained Call Rate	0
Maximum Egress Call Burst Size	0
Maximum Egress Sustained SIP nonInvite Rate	0
Maximum Egress SIP nonInvite Burst Size	0

The GSX Report window displays.

Report

Report Name:

Date Range: 07/30/2020 16:22:11 08/04/2020 16:22:11

Granularity: All

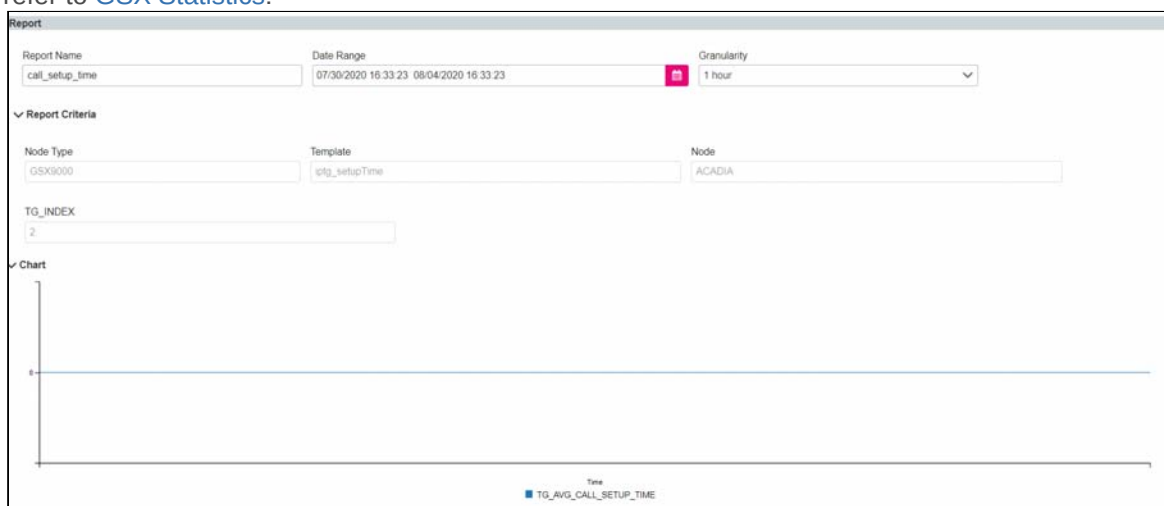
▼ **Report Criteria**

Node Type: Template: Node:

TG_INDEX:

Cancel Download | Run

8. In the **Report Name** field, enter a name for the report.
9. In the **Date Range**, set an interval:
 - a. Select an interval.
 - b. Click **Apply**.
10. From the **Granularity** drop-down menu, select one of the following granularity:
 - All
 - 1 Hour
 - 1 Day
11. Click **Run**. The PM chart and the table are displayed under the report. For more information on PM tables, refer to [GSX Statistics](#).



The screenshot shows the 'Report' configuration window in RAMP. It includes fields for 'Report Name' (cal_setup_time), 'Date Range' (07/30/2020 16:33:23 to 08/04/2020 16:33:23), and 'Granularity' (1 hour). Under 'Report Criteria', 'Node Type' is GSX0000, 'Template' is ipq_setupTime, 'Node' is ACADIA, and 'TG_INDEX' is 2. Below the criteria is a 'Stats Table' with columns 'TIMESTAMP' and 'TG_AVG_CALL_SETUP_TIME'. It displays two records for 08/04/2020. At the bottom are 'Cancel', 'Download', and 'Run' buttons.

TIMESTAMP	TG_AVG_CALL_SETUP_TIME
08/04/2020 12:30:00	0
08/04/2020 11:30:00	0

12. To download the report, click **Download**.
13. Select "Download PDF" or "Download CSV".
14. Click **Save**.

Historical Performance Charts

Historical Performance charts show performance data gathered over a designated time span as a sample graph.

When displaying a report, if you select a granularity value, the report displays a single bar for each period of time dictated by the granularity setting. For example, selecting a granularity of 1 hour results in the display of bars representing 1 hour intervals. At any time, to display the timestamp for a particular bar, hold the mouse on the bar in question and click. A popup field appears displaying the exact value and timestamp.

The Granularity determines how many points the system plots on the chart. If the data used represents counter values, then the Performance Manager accumulates the data, adds it together, for the time span. If the data used represents non-counter values, then the Performance Manager averages the data for the time span. For example, if you have the data collection set for 15 minute intervals and specify a one hour granularity, then the Performance Manager would add four rows of data for counter information, or average four rows for non-counter information. Use a smaller time interval to see greater detail. If you select a large time range, consider selecting a granularity option that reduces the number of data points displayed.

Note

Lines graphed for statistics with identical values appear as one plot/line since the second value is plotted over the first.

Event Log

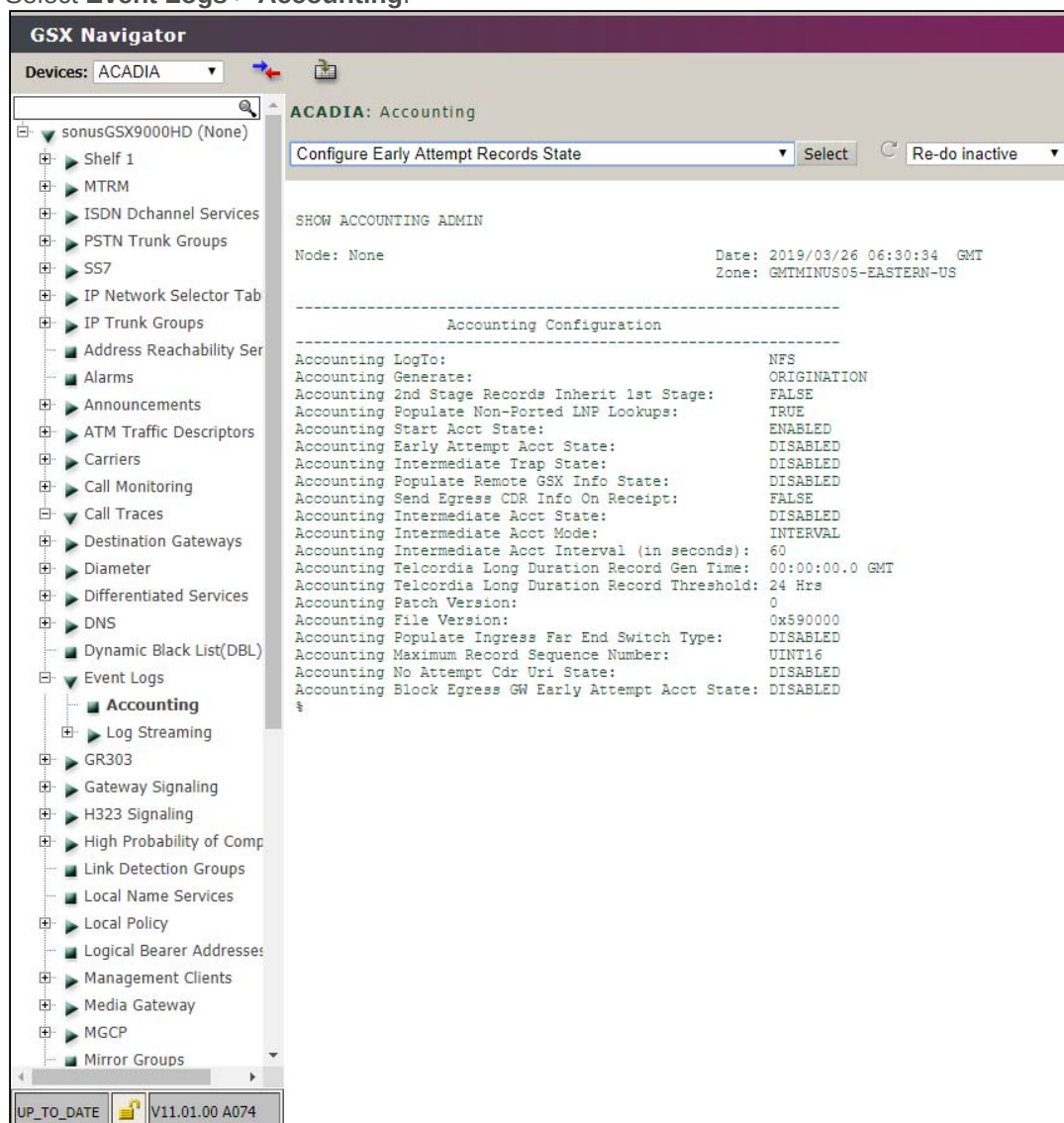
You can view and manage details or operations related to any GSX device registered on Ribbon Application Management Platform (RAMP).

Prerequisites

- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- Super User [privileges](#) for **Configuration Management** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.
- A GSX node is registered on RAMP.
- The GSX device is up and running.
- Data collection is enabled for the GSX node on RAMP.
- A trunk group is configured on the GSX.

Procedure

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the row for the GSX device you want to work with, click on the ellipses (...) menu and select **Configure**. The **GSX Navigator** window opens.
4. Select **Event Logs > Accounting**.



The following table lists Accounting operations supported through Event Logs.

Task Name	Task Description
Configure Early Attempts Record State	Specifies whether or not to generate early ATTEMPT records. An early ATTEMPT record is associated with an early call disconnect, before the policy request is sent.

Task Name	Task Description
Configure Early Attempts Record State At Egress Gateway	Specifies whether or not to block early ATTEMPT records at egress gateway. An early ATTEMPT record is associated with an early call disconnect, before the policy request is sent.
Configure Generate	Configures the type of calls for which accounting records should be logged on the GSX.
Configure Intermediate Records State	Configures the administrative state of accounting logging.
Configure Maximum Record Sequence Number	Specifies the maximum length of the Record Sequence Number field in the CDR.
Configure No Attempt CDR URI User State	Specifies whether or not to generate the ATTEMPT CDR URI records. The ATTEMPT CDR URI record is generated on termination of a call that was not complete
Configure Patch Version	Specifies the changes of the accounting patch version currently in use. This change takes effect immediately. The range is 0-255.
Configure Populate IP Trunk Group Ingress Far End Switch Type	Configures the ingress far end software type for IP Trunk group.
Configure Populate Non-porting LNP Numbers	Specifies whether an LNP lookup that returned the same number as the number that was searched on (or a nonported LNP number) should cause that number to be placed into the associated accounting record fields:
Configure Populate Remote-GW-Info	Specifies whether or not to correlate specific fields in the STOP and ATTEMPT accounting records on GSXGSX calls. The correlation is between the ingress (originating) GSX and the egress (destination) GSX.
Configure Populate Remote-GW-Info Send Immediate	Specifies whether to direct the originating GSX to immediately populate the Remote GSX Billing information from the egress GSX ready for inclusion in the next CDR record that is generated.
Configure Reset CDR Count	Resets the CDRs.
Configure Second Stage Inherit First	Specifies whether the second stage accounting record of a two stage call will inherit specific field values from the first stage of the call.

Task Name	Task Description
Configure Start Records State	Specifies whether or not to log START records.
Configure Summary Reset	Configures summary resets for accounting records.
Show Accounting Selectable CDR Population Record Type	Displays the CDR record type fields selected when using the Selectable CDR feature for Streaming Logging to the DSI
Show Accounting Selectable CDR Population Summary	Displays the summary of the CDR record type fields when using the Selectable CDR feature for Streaming Logging to the DSI
Show Accounting Selectable CDR Status	Displays the status CDR record type fields selected when using the Selectable CDR feature for Streaming Logging to the DSI.
Show Admin	Displays the accounting administrator profile.
Show Record Summary	Displays the accounting record summary.
Show Summary	Displays the accounting summary.

Verifying the Database Status

You can check the status of the Ribbon Application Management Platform (RAMP) database records for a selected GSX node using GSX navigator.

Prerequisites

- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- Super User [privileges](#) for **Configuration Management** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.
- A GSX node is registered on RAMP.
- The GSX device is up and running.
- Data collection is enabled for the GSX node on RAMP.
- A trunk group is configured on the GSX.

Procedure

1. Log on to the [RAMP GUI](#).
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the row for the GSX device you want to work with, click on the ellipses (...) menu and select **Configure**. The **GSX Navigator** window opens.
4. Click the "Report data collection" icon in the Toolbar to open the **Report Data Collection** window.
5. Select the **Report Database** tab and select the desired node in the **Select Node** field.

The **Database Status** field shows one of three states of the [RAMP](#) database for the selected node: up to date, out of date, or update in progress. Also listed are the sequence number of the last configuration parameter file written by the GSX and collected and stored by [RAMP](#), as are the timestamps of these events. If an update is in progress, the system displays additional information regarding the collection, processing and storage of the configuration data.

The **Refresh** button refreshes the dialog box. The **Collect Data** button triggers a request to collect configuration data from the GSX and process it.

Configuring GSX Call Trace Filters

To run a Call Trace report for GSX, you must first configure a Call Trace Filter using the GSX Navigator.

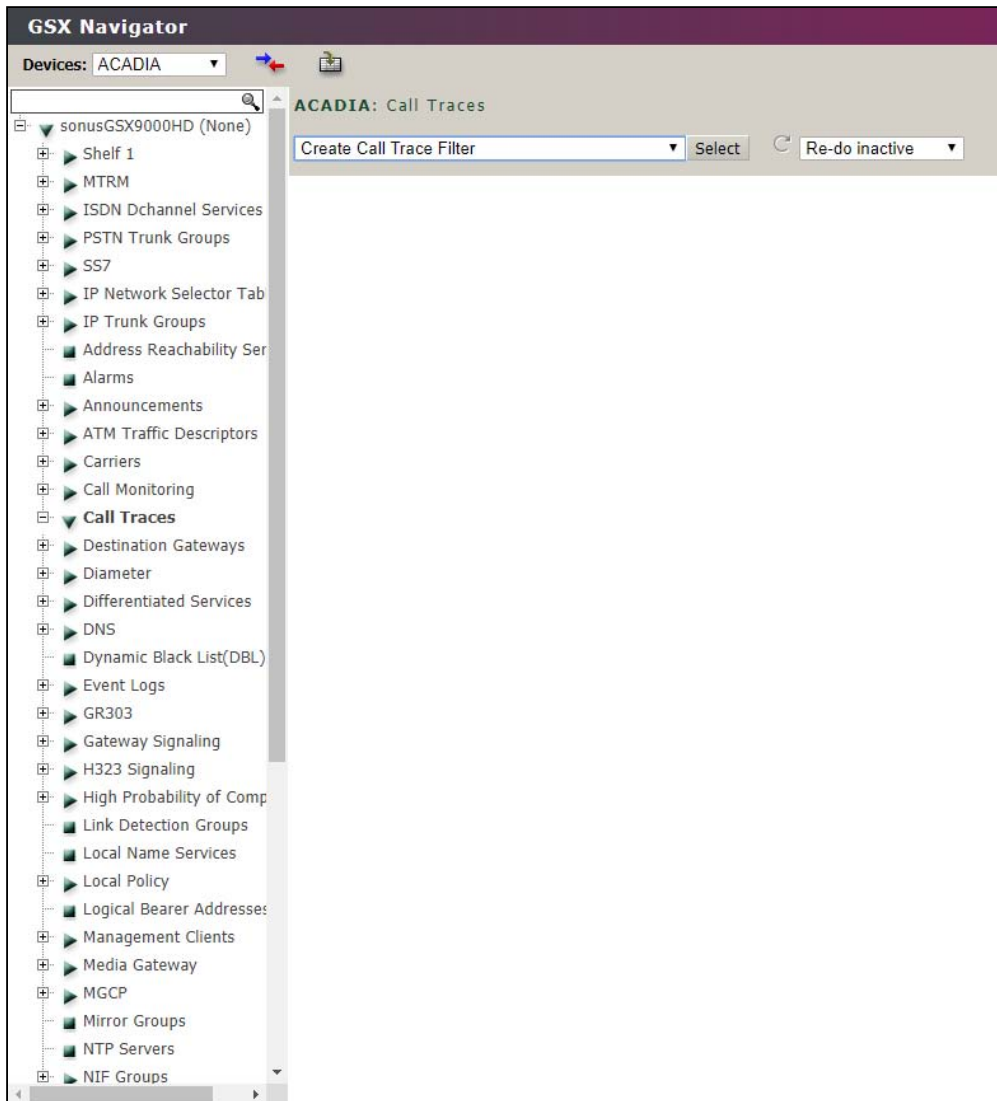
Use the following procedure to launch the GSX Navigator and configure a call trace filter.

Prerequisites

- The GSX device is registered on **RAMP**.
- The GSX device is up and running.
- GSX Provisioner or GSX Super User privileges.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- Super User [privileges](#) for **Configuration Management** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

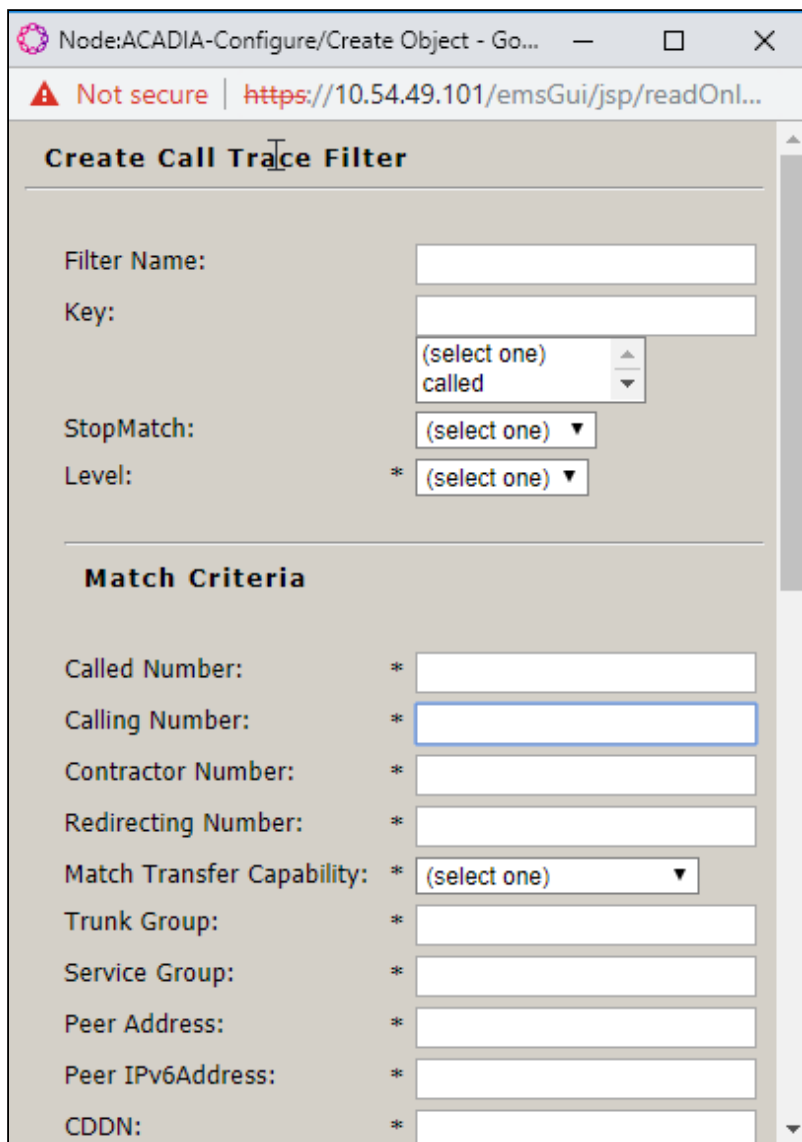
Start

1. Log on to the **RAMP** GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the row for the GSX device you want to work with, click on the ellipses (...) menu and select **Configure**. The **GSX Navigator** window opens.
4. Select **Call Traces** from the Node Objects tree. Expanding the tree shows any existing call trace filters.



5. Select **Create Call Trace Filter** from the Commands drop-down menu to set up a new call trace filter. The **Create Call Trace Filter** window opens.

Create Call Trace Filter



Node:ACADIA-Configure/Create Object - Go... — □ ×

⚠ Not secure | <https://10.54.49.101/emsGui/jsp/readOnl...>

Create Call Trace Filter

Filter Name:

Key:
called

StopMatch:

Level: *

Match Criteria

Called Number: *

Calling Number: *

Contractor Number: *

Redirecting Number: *

Match Transfer Capability: *

Trunk Group: *

Service Group: *

Peer Address: *

Peer IPv6Address: *

CDDN: *

6. Enter the appropriate parameters in the fields:
 - **Filter Name** — Enter a name for your call trace.
 - **Key** — From the list below the field select one or more (use CTRL + left click) options. Key options vary, depending on GSX version and may include: called, calling, cddn, contractor, gr303igcrv, peerIpAddress, redirecting, serviceGroup, slotPortChannel, transferCapability, or trunkGroup. The system populates the Key field based upon your selection(s).
 - **StopMatch** — Specifies whether to stop trying to match filter profiles after a match is found: unsupported (default) do not stop matching filter profiles after a match is found (up to three profiles will be matched), supported stop trying to match filter profiles after a match is found.
 - **Level** — There are three levels. Level 1 includes all call trace information, level 2 excludes raw hex dumps, and level 3 traces only external message information (ISDN/ISUP/CAS etc.) and errors.
7. In the **Match Criteria** section complete the necessary field based upon your Key setting. The fields are as follows:
 - **Called Number** — Enter the number called.
 - **Calling Number** — Enter the number placing the calls.
 - **Contractor Number** — Enter the contractor number.

- **Redirecting Number** — Enter the redirecting number.
- **Transfer Capability** — Select the transfer capability of the call to trace. Selections are: Speech, Unrestricted, Audio31KHz, unrestricted with tones, or Video.
- **Trunk Group** — Enter the name of a trunk group to trace. This string must match the trunk group name exactly. No wildcard characters allowed.
- **Service Group** — Enter the name of a service group to trace. This string must match the service group name exactly. No wildcard characters allowed.
- **Peer Address** — Enter the specific host IP Address of the source/destination of the call. For a P2P call, you must create two Call Trace Filters, if you wish to log the PDU for both call legs.
- **CDDN** — Enter the called directory number to trace.
- **GR303 Interface Group** — Enter the GR303 Interface Group to trace.
- **GR303 CRV (all or integer)** — Enter the Call Reference Value (CRV) within the named GR303 Interface Group. Or, enter all to trace an entire interface group.

If you selected **slotPortChannel** as the Key setting then specify one of the following groups of parameters as the Match Criteria:

- **Slot Number** — Enter the slot number on which to trace a call.
- **Port Number** — Enter the port or span supported by the module in the slot on which to trace a call.
- **Channel Number** — Enter the channel number (valid range is 132) on the slot/port on which to trace a call.
or
- **T1 Port Name** — Enter the name of the T1 span on which to trace a call.
- **Channel Number** — Enter the channel number (valid range is 132) on the specified T1 port on which to trace a call.
or
- **E1 Port Name** — Enter the name of the E1 span on which to trace a call.
- **Channel Number** — Enter the channel number (valid range is 132) on the specified E1 port on which to trace a call.

Note

When entering telephone numbers, do not use dashes, parentheses, spaces or other special characters. Use only numerals or wildcards. Use % as a substitute for trailing numbers and use an X (upper or lowercase) as a substitute for individual numbers. The examples below are for a 10 digit telephone number:

978683%

978xxx9455

61723489xx

8. Click **OK**.

In addition to viewing Call Trace reports for a GSX, you may view Call Trace information from PSX Policy servers. To configure Trace Destinations for PSX Policy Servers, refer to [PSX Call Trace Destination](#).

The system stores Call Trace data in Trace event logs. Each log has a maximum size of 2 MB. As the size of a log file increases above 2 MB, the system begins writing data to a new file. When the system has created the maximum number of trace files, new files overwrite older files.

Verify the log file size from the GSX Navigator by selecting the Event Logs category of the Object tree and then selecting Show Event Log All Admin from the Commands menu. You can change the number of files and file size on a temporary basis; however, once a GSX rediscovery occurs **RAMP** returns to its default setting of two 2 MB files. Ribbon recommends not to change the default settings.

Launch IDH GUI

Launch the Identity Hub Manager (IDH) GUI from Ribbon Application Management Platform (RAMP) to configure IDH devices.

Prerequisites

- The IDH device is registered on RAMP.
- Possess Super User [privileges](#) for GUI and Configuration Management under Core Resources.
- Possess **Devices** and **Resource Groups** [privileges](#) under Device Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list row for the STI device to configure, click on the ellipses (...) menu and select **Configure**. RAMP launches the IDH GUI.

For more information on configuring IDH devices, refer to [Identity Hub Manager on RAMP](#).

Launch L2MGR GUI

Launch the L2MGR GUI from Ribbon Application Management Platform (RAMP) to configure L2MGR devices.

Prerequisites

- The L2MGR device is registered on RAMP.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list, in the row for the L2MGR device you want to configure, click on the ellipses (...) menu and select **Configure**. RAMP launches the L2Mgr Cockpit GUI.
4. Log into the GUI using your login credentials.

For more information on configuring L2MGR devices, refer to [L2MGR Operations](#).

Launch PSX GUI

The Ribbon Application Management Platform (RAMP) provides access to the PSX Manager, PSX Manager Shadow, and the SoftSwitch Request (SSREQ) tools for use with the PSX devices registered on the RAMP.

- PSX Manager – The dedicated GUI for PSX through RAMP.
- SSREQ tool – Simulates call traces of PSX requests, such as policy, trigger, download, DIAMETER, and so on, to verify the provisioning of those features.
- PSX Manager Shadow – Use this tool to run PSX Manager against a PSX shadow database.

Prerequisites

- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.
- Access [privileges](#) to PSX Management.
- Java plug-in 1.8 or later on your personal computer (PC). For more information, refer to [PSX GUI launch using OpenJDK](#).
- TLS 1.2 is enabled on your personal work station.
- TLS 1.2 is enabled in your web browser.
- SSL 2.0 Compatible ClientHello Format is disabled.
- The RAMP IP address is added to the Exception Site List in the Java Control Panel on your Windows PC.
- Launch platforms and RAMP must be configured to perform FQDN to IP address resolution. For more information on PSX registration using an FQDN, refer to [Installing PSX SWe Instance using HEAT Templates](#).

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list, in the row for the PSX device you want to configure, click **Select Action** drop-down menu. The following options appear:
 - a. **Edit**
 - b. **Unregister**
 - c. **Delete**
 - d. **Launch PSX Manager**: To launch the PSX Manager. For more information on PSX Manager, refer to [PSX Manager User Guide](#).
 - e. **Launch PSX Manager Shadow**: To launch the PSX Manager for a shadow database. You are prompted to download a file <PSX name>.jnlp file.
 - f. **Launch SSREQ**: To launch the SSREQ tool. For more information on SSREQ, refer to [Using SSREQ Tool](#)
 - g. **Generate PSX Password**: To generate a new password for the PSX node.
4. Select **Launch PSX Manager** to launch the PSX Manager GUI.

PSX GUI launch using OpenJDK

The PSX manager is a Java Web Start (JNLP) application used to deploy Java applications over the web. Oracle deprecated Java Web Start with OpenJDK 9 and eventually removed it from OpenJDK 11 onwards. Thus, JNLP is not natively supported in OpenJDK versions 9 and above. However, you can still use JNLP with OpenJDK by using OpenWebStart, an open-source reimplementation of Java Web Start.

Start

Perform the following to launch a PSX Manager file using OpenWebStart with OpenJDK 9 and above on Windows.

1. Download [OpenJDK](#) from the official OpenJDK website. Run the installer and follow the setup wizard. Refer to the [System Requirements to Access RAMP on a Web Browser](#) for supported Java versions and Java distributions.
2. Install [OpenWebStart](#).

OpenWebStart is a free implementation of the Java Web Start technology, which was deprecated by Oracle in JDK 9.

3. Run the installer and follow the setup wizard.
4. Ensure that the `OpenWebStart` is associated with '.jnlp' files, during the installation.
5. To configure the `OpenWebStart` with OpenJDK9,
 - a. Open the `OpenWebStart` settings via the Start Menu or by launching the `OpenWebStart Settings` application.
 - b. Go to Java Virtual machine (JVM) manager tab in the Settings.
 - c. To add a new JVM, click **Add local**.
 - d. Browse the directory where the Open JDK 9 is installed. Select the `java.exe` or `javaw.exe` file in the `bin` directory.
 - e. After adding, set this as a default JVM or select when launching a JNLP file.
6. To launch the **PSX Manager**, double-click or right-click the JNLP file and choose Open with `OpenWebStart`. The `OpenWebStart` launches the application using the specified OpenJDK version. For more information on PSX Manager launch, refer to [Launch PSX GUI](#).

Launch SBC Core and SLB GUIs

Related articles:

- [Mapping Between RAMP and SBC User Privileges](#)

Ribbon Application Management Platform (RAMP) supports launching graphical user interfaces (GUIs) to configure manually registered SBC and SLB nodes.

When you select the option to configure an SBC Core or SLB device, RAMP launches either the **Ribbon** SBC Configuration Manager or SLB Configuration Manager application, as appropriate. The SBC/SLB Configuration Managers provide options similar to the SBC Embedded Management Application (EMA). For more information on EMA, and configuration procedures, refer to the [EMA User Guide](#).

Note

If you have launched the SBC/SLB Configuration Manager for a device, do not launch the SBC/SLB Configuration Manager for another device until the first instance is completely loaded.

Prerequisites

- The SBC Core/SLB device is registered on RAMP.
- Provisioner or Super User [privileges](#) for **Configuration Management** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

To update the configuration for an SBC/SLB device:

1. Log on to the [RAMP](#) GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window opens.

3. In the nodes list row for the SBC/SLB device you want to configure, click on the ellipses (...) menu and select **Configure**. RAMP launches the appropriate GUI for the device.

Note

You can view or edit CALEA configuration through the SBC/SLB Configuration Manager if the RAMP user account with which you are logged in has CALEA privileges.

4. After you complete your configuration changes on SBC/SLB Configuration Manager, click **Save and Activate**.

Mapping Between RAMP and SBC User Privileges

When you access the Ribbon SBC Configuration Manager from RAMP, the privilege levels set for Insight Administration, GUI, and Authentication and Authorization applications determine access permissions. Refer to [Set Privileges for Users by Adding Roles](#) for additional information.

The application-level privileges in RAMP correspond to user roles in SBC. Refer to [Managing SBC Core Users and Accounts](#) for additional information.

The mapping between the RAMP application-level privileges and SBC user roles is as follows.

Mapping RAMP application privileges to SBC user roles

Application (RAMP)	privilege	corresponding SBC user role
Insight Administration	Super User	Administrator
GUI	Super User	Access to GUI
Authentication and Authorization	Super User	Calea
Only when logged in as the "Calea" user.		

Launch SBC Edge GUI

Launch the SBC Edge GUI from Ribbon Application Management Platform (RAMP) to configure SBC Edge devices.

Prerequisites

- The SBC Edge device is registered on RAMP.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.

2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list, in the row for the SBC Edge device you want to configure, click on the ellipses (...) menu and select **Configure**. RAMP launches the SBC Edge GUI for the device.
4. Log into the GUI using your SBC Edge login credentials.

For more information on configuring SBC Edge devices, refer to [SBC Edge Documentation](#).

Launch SGX GUI

Launch the SGX Manager GUI from Ribbon Application Management Platform (RAMP) to configure and view SGX objects.

You can issue commands and change parameter settings by first selecting the applicable parent/child object in the object tree in the left pane. Once you select an object, the fields associated with the object appear in the right pane along with action buttons that you click to perform an action.

For more information refer the [SGX 10.0.x Documentation Home](#).

Prerequisites

- The SGX device is registered on RAMP.
- The SGX device is up and running.
- You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

To launch a node after registering in RAMP:

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list, in the row of the registered SGX device you want to configure, click on the ellipses (...) menu and select **Configure**. The SGX Manager window opens.

Note

User access from CLI or RAMP is disabled (and forcefully disconnected) at system startup when CE1 begins its connection to CE0. You may notice this if you connect too soon to a system that is restarting. The disconnect is only temporary; you will see the message "Stopping user sessions during sync phase!" when this situation occurs.

Launch STI GUI

Launch the Secure Telephony Identity (STI) GUI from Ribbon Application Management Platform (RAMP) to manage STI devices.

Prerequisites

- The STI device is registered on RAMP.
- Possess Super User [privileges](#) for GUI and Configuration Management under Core Resources.
- Posses **Devices** and **Resource Groups** [privileges](#) under Device Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**. The **Devices** window displays.
3. In the nodes list row for the STI device to configure, click on the ellipses (...) menu and select **Configure**. RAMP launches the STI GUI.

For more information on configuring STI devices, refer to [Accessing STI Manager from RAMP](#).

Work with Resource Groups

In this section:

- [Create a Resource Group](#)
- [Edit a Resource Group](#)
- [Delete a Resource Group](#)

A Ribbon Application Management Platform (RAMP) resource group is a collection of nodes and clusters that are managed primarily for the purposes of access control.

A resource group defines a logical partition of either individual devices or device types. These groupings participate in a three-way relationship with roles and user groups to fully define user access to devices registered on RAMP, and to particular management functions.

This ensures that each user group has access to the appropriate resource group for their region and the proper privileges (role) for provisioning the PSX. For more information, refer to [Set Privileges for Users by Adding Roles](#).

For example, if you have users whose sole responsibilities are to provision PSXs where:

- a subset of users are responsible for PSXs in the Northern region,
- another subset provision PSXs in Southern region, and
- a manager is responsible to oversee all PSXs,

you can create three resource groups (For example, PSX_North, PSX_South, and PSX_All).

Within RAMP Device Management, you can use the characteristics of resource groups to bring efficiency to your operations. If your network of managed devices is subject to change, you can use configuration options to minimize the impact of adding new devices. For example, if you create a resource group that is dedicated to managing a particular type of device, you can specify in the parameters of the resource group that you want new devices of that particular type automatically added to the resource group. Similarly, when adding new devices to RAMP, either through individual device registration or when adding a cluster, you have the option to select a resource group to which you want to add the new device. Either of these configurations can help you avoid having to update the resource group itself to add the device.

Note that you have the option to define resource groups by specifying a "parent-child" relationship for a resource group. A parent resource group automatically includes all of the devices in any child resource groups for which it is the parent. A hierarchy of this type can have up to five levels.

Except for SBC Edge, devices can belong to multiple resource groups. An SBC Edge device must belong only to a single resource group in order to generate correct billing for SBCaaS.

Create a Resource Group

Use the following procedure to create a resource group.

Prerequisites

Devices and Resource Groups [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Resource Groups**. The "Resource Groups" window displays.
3. Click **Add Resource Group**. The "Add Resource Group" window displays.
4. Use the following (Resource Group Parameters) table to configure resource group parameters and then click **Save**.
5. To add a new resource group to a user group, refer to [Add User Groups](#).

Resource Group Parameters

Parameter	Description	Value range	Mandatory/Optional
Resource Group Information			
Resource Group Name	Enter a name for the resource group.	Up to 20 alphanumeric characters. The space character and special characters are not allowed.	M
Tenant	Used to implement multi-tenancy. The default value is root. For more information on multi-tenancy, refer to Configure Multi-Tenancy .		M
Description	Enter a description for the resource group.		O
Parent Resource Group	Select a resource group if you want to assign a parent group to the new resource group. The parent resource group automatically contains all of the devices within its child resource groups. The parent-child hierarchy of resource groups is limited to 5.		O
Automatic Device Association			
Note When you select a clustered node type and add or edit a resource group for Automatic Device Association, RAMP automatically associates all the non-cloud nodes, clusters along with its associated nodes to the resource group. For example, in Automatic Device Association, under Type, if you select All PSX Devices, then the non-cloud PSX nodes, cloud PSX nodes and the PSX cluster are automatically associated to the resource group.			

Parameter	Description	Value range	Mandatory/Optional
Type	Select one or more types of devices (nodes or clusters) that you want to include in the resource group. Your selection automatically adds devices of the selected types to the "Selected" lists under Manual Device Association. This control provides a simple way to add multiple nodes or clusters to the selected list. Note that you can still use the arrow controls to move individual nodes, or all nodes, between the lists.	The list of node and cluster types currently present on your RAMP system.	O
Manual Device Association Note Ramp lists only non-cloud nodes when you add or edit a resource group using Manual Device Association. When you associate a cluster to a resource group, RAMP automatically associates all the nodes in that cluster to the resource group.			
Available Nodes	Use the controls in the Manual Device Association section to specify which devices the resource group contains. From the Available Nodes and Available Clusters lists, select devices you want to include in the resource group and use the right arrows to move them to the Selected Nodes and Selected Clusters lists. Devices you include in the Selected lists are part of the resource group.	The list of nodes currently registered on your RAMP system.	
Available Clusters	Use the left arrows to move devices back to the Available Nodes and Available Clusters list if you do not want to include them.	The list of clusters currently registered on your RAMP system.	
Selected Nodes	Note that if any of the lists of devices is long, you can enter text at the top of the list to filter the device list to include only devices with device names that include the filtering text.		
Selected Clusters			

Edit a Resource Group

You can edit an existing resource group to change parameters or to add or remove nodes and clusters.

Start

1. Log on to the Ribbon Application Management Platform GUI.

2. Navigate to **DEVICE MANAGEMENT > Resource Groups**. The "Resource Groups" list window opens.
3. In the row for the resource group, click the pencil icon under **Actions** to open an edit window. Note that some parameters can no longer be changed.
4. Refer the previous table for parameters and click **Save**.

Delete a Resource Group

You can delete a resource group that is no longer needed.

Start

1. Log on to the Ribbon Application Management Platform GUI.
2. Navigate to **DEVICE MANAGEMENT > Resource Groups**. The "Resource Groups" window displays.
3. In the row for the resource group, click the delete icon under **Actions**.
4. Confirm the deletion when prompted.

Work with Inventory Reports

In this section:

- [Create an Inventory Report](#)
- [Edit an Inventory Report](#)
- [Run an Inventory Report](#)
- [Delete an Inventory Report](#)
- [Network Summary Report](#)

Ribbon Application Management Platform (RAMP) retrieves inventory details for SBC Core, SBC Edge, DSC and SLB devices. The inventory details provide a range of data including information on hardware, software, firmware, ports, and licenses. The specific information available depends on the type of device.

You can retrieve inventory information on one or more devices using Inventory Reports. In the report parameters, you specify the devices to include and the type of information you want to retrieve. You can download the reports in different formats and export them. You can save sets of Inventory Report parameters to be able to run them again or to schedule them to be run regularly.

Create an Inventory Report

You can create inventory reports for SBC Core, SBC Edge, DSC, and SLB devices.

Prerequisites

- Devices are registered on RAMP.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices, Inventory Reports, and Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Inventory Reports**.
3. Click **Add Report**. The **Add Report** window displays.
4. Use the following table to configure the report parameters and then click **Save**.

Inventory Report Parameters

Parameter	Description	Range
Details		
Name	Enter a name for the report.	Minimum of five characters.
Description	(Optional) You can provide a description of the report.	
Devices		
Tenant	Used to implement multi-tenancy. The default value is root. For more information on multi-tenancy, refer to Configure Multi-Tenancy .	
Device Type	Select one or more device types to include in the report. Your choice of device types populates the Available device list.	• DSC • SBC Core • SBC Edge • SLB
Available Device	Use the arrows to move devices you want to include in the report from the Available list to the Selected list. You can select multiple devices.	
Selected Device	Displays the devices you selected from the list of Available list. This is the list for which the inventory report is generated.	
Columns		

Parameter	Description	Range
Include Inventory Groups	Use the controls in the Columns section to specify the inventory data you want to include in the report. RAMP divides inventory output into different categories called “inventory groups.” When you create a report, the list of inventory groups available depends on the type of devices you select.	• Feature Licenses • System Inventory • Node Modules • Ports • Port Licenses • Part Inventory • Slot Inventory
Available Columns	From the Include Inventory Groups list, select one or more inventory groups to add the associated inventory parameters to the Selected Columns list. Items you include in the Selected list appear in the Inventory Report. Use the arrows to move columns you do not want to include in the report to the Available list. Note that if the list of columns is long, you can use the Column and Groups fields to locate matching items in the list.	
Selected Columns		
Frequency, Format, and Location		
Frequency	Select when to generate the report. • Now - The report is generated immediately. • Later - Select the date and time for the report to be generated. • Repeat - Select how frequently you want the report to be auto-generated. ◦ Daily - Select the time at which the report is to be generated every day. ◦ Weekly - Select the day of the week and time at which the report is to be generated every week. ◦ Monthly - Select the day of the month and time at which the report is to be generated monthly.	• Now • Later • Repeat
Format	Select the format in which you want the report to be generated.	• HTML • CSV • XML • PDF

Parameter	Description	Range
Location	Select whether you want to download the report or export it. • Download - The report is downloaded to the local machine. • Export - Provide a location for the report to be exported.	• Download • Export
Export Locations	These parameters are applicable only when you choose Export. You will see a message: Report export initiated successfully. For export report log, check /opt/sonus/pm/logs/pm_copier_service_trace_log. If the export is a failure, the sonusEmsPMExportSFTPFailNotification alarm is raised. For logs, see /opt/sonus/pm/logs/pm_copier_service_trace_log • Select Localhost to download the report to the local machine. The IP Address and Directory are automatically populated. • To send the report to a remote location, enter the IP Address for the remote server and a Directory name where you want to store the report. Enter the Username and Password needed to access the remote server.	• Localhost • <any other location>

Edit an Inventory Report

You can edit an existing inventory report to update its parameters.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Inventory Reports**. The Inventory Reports list window opens.
3. In the row for the report you want to edit, select the pencil icon under **Actions** to open the edit report page.
4. Edit the report as needed. Refer to the previous table for parameters.

5. Click **Save**.

Run an Inventory Report

Run an Inventory Report report to gather updated information for specified devices.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Inventory Reports**.
3. In the row for the report you want to run, select the play icon under **Actions**.

Delete an Inventory Report

You can delete a report that you no longer need.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Inventory Reports**.
3. In the row for the report you want to delete, select the delete icon under **Actions**.
4. Confirm the deletion when prompted.

Network Summary Report

The Network Summary Report contains the node name, version, and count of the nodes in a network. This report is not available in the RAMP GUI.

Note

The NetworkSummaryReport is scheduled to run everyday at 2 A.M. The report is saved in a CSV format in `/opt/devMgmt/reports/inventory/inventoryReports`. It contains the node name, version, and count. The report is not available in the UI.

Modify Managed Device Association

Use the **Managed Device Association** window to change the IP address with which devices are associated for Ribbon Application Management Platform (RAMP) services. For example, you could make this type of change to temporarily associate the set of devices currently registered with one RAMP instance with another RAMP instance, while you upgrade the original instance. Or, you could use this option to associate devices with a new RAMP IP address if it must be changed. You can also use these options when migrating devices from one RAMP instance to another.

When you associate devices with a specified RAMP IP address, it establishes a communication path between the devices and that RAMP, enabling the flow of management and alarm information. When you disassociate devices with an IP address you remove the management relationship between the devices and the corresponding RAMP. Disassociation might be needed if you remove a RAMP instance from the network or to complete a switch back to an upgraded instance.

Use the following procedure to access the **Managed Device Association** window to make changes to device association with RAMP.

Prerequisites

- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices, Inventory Reports, and Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log onto the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. In the upper-right corner of the window, click the three dots adjacent to **Add Device** to open a menu where you can select **Managed Device Association**. The **Managed Device Association** window opens.
4. In **IP Address**, enter the IP address of a RAMP instance you want to either associate or disassociate from the currently registered devices.
5. Click **Associate** or **Disassociate**, as appropriate.

Note that you can also access the **Managed Device Association** window from the **Resource Groups** and **Inventory Reports** windows under **Devices**.

Configure Device Management Administration Options

Ribbon Application Management Platform (RAMP) Device Management provides an **Administration** window where you can specify options that tailor the operations of Device Management services to your specific environment.

Prerequisites

- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices, Inventory Reports, and Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. In the window's upper-right corner, click the three dots adjacent to **Add Device** to open a menu where you can select **Administration**. The **Administration** window opens.
4. Use the following table to configure the parameters and click **Save**.

Device Management Administration Parameters

Parameter	Value Range	Description	Mandatory
Application Management - Node			
Node status history purger task start time		Specifies the time to purge the node status history everyday. The must be specified in <hh:mm:[AM/PM]>.	No
Node status history retention period (in days)		Specifies the number of days after which the node status history data will be purged.	No
Application Management - Cluster			
Cluster Configuration limit enabled	• Enable • Disable	Enable this option to activate the limit on the number of configurations RAMP stores for a cluster. By default, this option is enabled.	No

Parameter	Value Range	Description	Mandatory
The max number of cluster configurations stored	1 - 200	Specifies the number of configurations that can be stored for a cluster on the system. If you store more than the configured maximum, older configurations are overwritten by new configurations. The default value is "50".	✓
Application Management - Inventory			
Inventory Collection	• Enable • Disable	Enable this option to activate inventory collection on RAMP. By default, this option is enabled.	No
Inventory Collection on Discovery	• Enable • Disable	Enable this option to enable collecting inventory data during node discovery. By default, this option is enabled.	No
Inventory Data purge period	1 day - 4 weeks	Select the number of days or weeks after which you want purge inventory data. The default value is "6 days".	✓
Application Management - Reachability Polling			
Max number of concurrent reachability tasks	30 - 100	Select the number of reachability tasks that can be running concurrently. In large networks where RAMP is frequently polling many devices, it may be necessary to increase this limit. After changing the limit, restart the reachability process to have the new limit take effect. The default value is "50".	✓
SNMP Client Retries	1 - 3	Select the number of times to retry an SNMP request before timing out. The default value is "1".	✓
SNMP Client Timeout	• 500ms • 1s • 5s • 10s	Select the number of seconds before a confirmed SNMP request is resent or timed out. The default value is "500ms".	✓

Parameter	Value Range	Description	Mandatory
REST Client Connection Pool Size	10 - 1000	Select the number of connections allowed in the REST client connection pool. After changing the limit, restart the reachability process to have the new limit take effect. The default value is "500".	✓
REST Client Connection Pool Size per Route	1 - 3	Select the number of REST client connections allowed per URL. After changing the limit, restart the reachability process to have the new limit take effect. The default value is "2".	✓
REST Client Establish Connection Timeout	5 - 120	Select the number of seconds to allow RAMP to make the initial socket connection to a device.the connection is timed out. After changing the limit, restart the reachability process to have the new limit take effect. The default value is "60".	✓
REST Client Socket Timeout	5 - 120	Select the number of seconds the REST client socket can be inactive before timing out. After changing the limit, restart the reachability process to have the new limit take effect. The default value is "60".	✓
Multiple GSX Navigator Windows Configuration			
Maximum Number of GSX Navigator Windows	1 - 10	Select the number of GSX Navigator windows that can be open simultaneously. The default value is "3".	✓

Firmware Repositories

The Ribbon Application Management Platform (RAMP) supports adding new firmware repositories.

Prerequisites

- **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.

- **Devices, Resource Groups, Firmware Repositories, and Job Status** [privileges](#) under **Device Management**.

Perform the following procedure to add a firmware repository. To add a firmware repository to a resource group, create an EdgeMarc profile and associate the firmware repository. For more information on creating EdgeMarc profiles, refer to [Manage EdgeMarc Profiles](#).

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Firmware Repositories**.
RAMP displays the **Firmware Repositories**.
3. Click **+ Add Repository**.
RAMP displays the Add Repository window.
4. Use the following table to create a firmware repository and click **Save**.

Parameters to create a Firmware Repository

Parameter	Description	Length/Range
Details		
Repository Name	Provide a name for the firmware repository.	1-128 alphanumeric characters
Type	Select the type of firmware repository you are creating. • FTP • SCP The default value is "SCP".	
IP/FQDN	Provide the IP address or the FQDN.	
Base Path	Provide the base path to create the firmware repository.	
Username	Provide a user name.	1-98 alphanumeric characters
Password	Provide a password.	1-96 alphanumeric characters
Available	Lists the available firmware versions. Select one or more firmware versions and click > or >> to move the selected firmware version(s) to the Selected table.	
Selected	Lists the selected firmware versions. To deselect one or more firmware versions click < or << to move the firmware version(s) back to the Available list.	

Parameter	Description	Length/Range
Get Latest Versions	Click Get Latest Versions to get the latest available firmware versions. This is updated in the Available list of firmware versions.	
Upload Firmware Versions	Click Upload Firmware Versions to upload from your local system.	

Device Operations

In this section:

- [GSX CLI Through RAMP](#)
- [Enabling Deprecated Algorithms for RAMP CLI](#)
- [RESTCONF API for SBC Core](#)
- [SOAP API for SBC Core](#)
 - [API Web Services for SBC](#)
 - [Writing an Insight API Client for SBC](#)
 - [API Error Handling for SBC](#)
 - [SBC Provisioning Operations](#)
- [SOAP API for PSX](#)
- [PSX CLI Through RAMP](#)
- [SBC CLI Through RAMP](#)
- [Provision SBC Devices](#)
 - [Provision SBC Core](#)
 - [Compare Uploaded Configurations for SBC Core or SLB Devices](#)
 - [Provision SBC Edge Devices](#)
- [Back Up and Restore SBC and SLB Devices](#)
 - [Take Backup of SBC Edge Devices](#)
 - [Take Backup of SBC Core and SLB Devices](#)
 - [SBC Edge Devices Catalog Management](#)
 - [SBC Core and SLB Catalog Management](#)
 - [Backup Catalog](#)
- [Upgrade SBC Devices](#)
 - [Upgrade SBC Core](#)
 - [Upgrade SBC Edge](#)
 - [Upgrade SLB](#)
- [Generate Health Reports](#)
- [Lock and Unlock Devices](#)
- [Automate Configuration Tasks for GSX](#)
 - [Task Definitions](#)
- [GSX Upgrade Automation](#)

Ribbon Application Management Platform (RAMP) Operations provide a range of functions for managed devices including provisioning, backup, upgrade, health reports, device locking, and access to a device's CLI. The types of operations that apply depend on the type of device.

GSX CLI Through RAMP

- [Entering GSX CLI Commands](#)

Entering GSX CLI Commands

The Ribbon Application Management Platform (RAMP) CLI supports entering GSX commands.

Perform SSH through port 8122 to enter GSX commands from the RAMP CLI.

Note

The idle timeout interval for a CLI session is set to 30 minutes.

Prerequisites

- You must have **Super User** [privileges](#) for **CLI** under **Core Resources**.
- The GSX device is registered on RAMP.
- The SSH client supports at least one of the following Ciphers/Kex/MACs:
- Ciphers:

```
aes-192ctr
```

- Kex:

```
ecdh_sha2_nistp384  
ecdh_sha2_nistp521  
diffie_hellman_group14_sha1  
diffie_hellman_group14_sha256
```

- MACS:

```
hmacsha256  
hmacsha512
```

- (Optional) To enable the deprecated algorithms for RAMP CLI, refer to [Enabling Deprecated Algorithms for RAMP CLI](#).

Start

1. Enter the following command on a Linux server:

```
ssh -p 8122 <RAMP username>@<RAMP ID address>
```

The following is an example:

```
ssh -p 8122 cliuser@10.11.22.33
```

The following message displays:

```
The authenticity of host '[<RAMP ID address>]:8122 ([<RAMP ID address>]:8122)'
can't be established.
RSA key fingerprint is <fingerprint>.
Are you sure you want to continue connecting (yes/no)?
```

2. Enter "yes". The following message displays:

```
Warning: Permanently added '[<RAMP ID address>]:8122' (RSA) to the list of known
hosts.
Password authentication
Password:
```

3. Enter the password. The following message displays:

```
Sonus Insight

Sonus Insight Command Line Interface
Date: <date and time>
```

4. Enter the following command:

```
f t i
```

The following is a sample output:

```
Target           : GSX
Target Version    : V14.00.00
Target Instance   : GSX
Target Instance Version: V14.01.00R000
```

5. Enter the following command:

```
s t i <name of the instance>
```

Example:

```
s t i GSX
```

The following is a sample output:


```
Result: Ok
GSX:V14.00.00R000:GSX>
```

6. Enter the commands for the GSX device. For information on GSX CLI commands, refer to [GSX9000 Operations and CLI Reference](#).

Enabling Deprecated Algorithms for RAMP CLI

The RAMP routinely phases out cryptographic algorithms that are deemed insecure or vulnerable by contemporary standards. Due to their vulnerabilities, the following cryptographic algorithms are disabled by default in RAMP. By disabling these algorithms, only more secure encryption methods and modes are utilized for SSH connections. This enhances the overall security of the SSH protocol by preventing potential exploits that could compromise data integrity and confidentiality. You can enable less secure cryptographic settings for the RAMP CLI by modifying the `Listener.properties` file.

Enabling less secure cryptographic ciphers, MACs, or key exchange (KEX) algorithms in SSH can expose your system to multiple security vulnerabilities.

Perform the following procedure to enable the deprecated Algorithms for RAMP CLI.

Start

1. Access RAMP as the `insight` user. Refer to [Log onto the RAMP CLI](#) to access RAMP as the `insight` user.
2. To enable the deprecated `ciphers`, `macs`, and key algorithms, include the below line in the `/opt/rbbn/ems/weblogic/sonusEms/data/cli/framework/resources/Listener.properties`.

```
com.sonus.cli.framework.ciphers=aes128cbc,aes128ctr,aes256ctr,aes192cbc,aes192ctr,
aes256cbc

com.sonus.cli.framework.macs=hmactsha256,hmactsha512,hmactmd5,hmactmd596,hmactsha1,hmact
sha196

com.sonus.cli.framework.kex=ecdhp256,dhg14,dhg14_256,dhg1,ecdhp384,ecdhp521
```

3. Restart the RAMP. For more information, refer to [How to Start and Stop RAMP](#).

RESTCONF API for SBC Core

The Ribbon Application Management Platform (RAMP) Representational State Transfer Configuration (RESTCONF) APIs for SBC Core are a collection of Web APIs (or Web Services) conforming to the REST architectural style.

Note

The RAMP SBC API Proxy only supports SBC Core version V11.01.00 and above.

Note

The `proxyAdminUser` and `netconf` user configured in Device Management should match; if not, the API fails.

The command `show table system ssoAuth proxyAdminUser` to check `proxyAdminUser` is configured on the SBC side.

You can perform look-up, create, modify and delete on the resources in SBC Core. The response to a REST request will be in XML format with a status block and a resource block where applicable.

The Authentication & Authorization section of RAMP is enhanced with the addition of the SBC Provisioning Role to control RAMP user privileges in the SBC provisioning role when accessing SBC's REST API and CLI.

The host IP address in the REST API requests is replaced with the RAMP IP address. Additional context "sbxProxy" and the registered node name of the target SBC Core are added to the URL.

Before making an SBC API call through the RAMP proxy as a RAMP user, the user needs to first ask for a JWT token from RAMP's Authentication & Authorization.

Here's the syntax depicting a token request for RAMP. You must be logged in as an admin user and use the curl tool as the client.

```
curl -d '{"userName":"admin","password":"admin"}' -k -H 'Accept: application/json' -H 'Content-Type: application/json' -X POST https://<RAMP_IP>/auth/v1.0/session/password
```

An example, this is a token request to RAMP server 10.34.146.120. The JWT token string is returned by RAMP Authentication & Authorization:

```
curl -d '{"userName":"admin","password":"admin"}' -k -H 'Accept: application/json' -H 'Content-Type: application/json' -X POST https://10.34.146.120/auth/v1.0/session/password {"token":"eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhZG1pb2IiInVzZXJHcm91cHMlOiYWRtaW4iXSwidGVuYXV5W50SWQ0IzODQwMDAwMC04Y2YwLTExYmQtYjIzZS0xMGI5NmU0ZWYwMGQiLCJ1dWlkIjoiodDhhOTM1ZGUtZTkzM00MzFhLTkzYjctNzFmYjM4N2Q4NDJiIiwiaWF0IjoxNzE5NTYwOTE5LCJleHAiOjE3MTk1NjE4MTl9.rV2VvBnlFvfjpTDgyYihu-USFT060iIn5ZpA_FJ38J9v9nJIaTGXzFuCsJkofsFqBvPtLEKlMj8TkT_s26rs_lBKeYTWJpsTrbZhGI3a-
```

```
curl -H Authorization:<TOKEN_STR> -XGET -i https://<RAMP_IP>/sbxProxy/<SBC_NAME>/restconf/data/<SBC_API_URL> --insecure
```

```
# curl -H
Authorization:eyJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJhZG1pb2IiInVzZXJHcm91cHMlOlsiYWRTaW4iXSwidGVuYW50SWQ0IiZiODQwMDAwMC04Y2YwLTExYmQtYjIzZS0xMGI5NmU0ZWYwMGQlLCJldWlkIjoieY2VhZDkyMDAtYTIxYS00ZDUzLWFiNWEtZmQwNjM1ZTY4OGIyIiwiaWF0IjoxNzE5NTY0ODA2LzJleHAiOjE3MTk1NjU3MDZ9.bIWz8I70r8TiiP9y72tzFdnYBXz15Y9L1oQcWYspo6k4qyZNmNH0wwUKBgYPFeM2G0_m5b0AqIQx0Hz112Rfc0mc5R9LcvN2vMxuQ5FVHp31AkIXtloRgAVtTI-
pPFveeFmnkhTB7k_S-9Im8FhvVCMEzwpb0A0iE1YfBsle4CI7MoZveTmlCoDiYyl7gWKb4P7_NAaRBcJFUaUuEE
--
hLo0xWXot4140YDyeYPxhr6xemgXTXrpgJshYr7tiEYpXODFaBiyliaZCcegFLPUgN6EUxsSA5PNdX3FVuhiZaih
Lba5mHSWU0g8By0cvRULFry5b5D1fxd8bPQX4qWwA -XGET -i https://10.34.146.120/sbxProxy/
directIntegrated/restconf/data/sonusAddressContext:addressContext=democontext --insecure
HTTP/1.1 200
Date: Fri, 28 Jun 2024 08:54:35 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, DELETE, PUT, OPTIONS, HEAD
Last-Modified: Fri, 28 Jun 2024 07:51:53 GMT
Access-Control-Allow-Headers: Content-type, origin, accept, authorization
Access-Control-Allow-Credentials: true
Content-Security-Policy: default-src 'self' blob: data: 'unsafe-eval' 'unsafe-inline';frame-ancestors 'self';
Content-Type: application/yang-data+xml
Via: 1.1 cisdCmpRestmicroEMS
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: master-only
Strict-Transport-Security: max-age=31536000, includeSubDomains, preload
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
Transfer-Encoding: chunked

<addressContext xmlns="http://sonusnet.com/ns/mibs/SONUS-ADDRESS-CONTEXT/1.0"
xmlns:ADDRESS_CONTEXT="http://sonusnet.com/ns/mibs/SONUS-ADDRESS-CONTEXT/1.0">
```

```

<name>democontext</name>
<ipRouteStatus xmlns="http://sonusnet.com/ns/mibs/SONUS-IP-ROUTE/1.0">
<ceName>intActive-192.168.1.22</ceName>
<destIpAddress>0.0.0.0</destIpAddress>
<prefix>0</prefix>
<nextHop>10.34.146.1</nextHop>
<ipInterfaceName>mgt0</ipInterfaceName>
<protocol>other</protocol>
</ipRouteStatus>
<ipRouteStatus xmlns="http://sonusnet.com/ns/mibs/SONUS-IP-ROUTE/1.0">
<ceName>intActive-192.168.1.22</ceName>
<destIpAddress>10.34.146.0</destIpAddress>
<prefix>23</prefix>
<nextHop>0.0.0.0</nextHop>
<ipInterfaceName>mgt0</ipInterfaceName>
<protocol>other</protocol>
</ipRouteStatus>

.....
<sipSubCountStatistics xmlns="
http://sonusnet.com/ns/mibs/SONUS-SIP-SUB/1.0">
<name>entry</name>
<sipSubCountAttempts>0</sipSubCountAttempts>
<sipSubCountCumCompletions>0</sipSubCountCumCompletions>
<sipSubCountStable>0</sipSubCountStable>
<sipSubCountFailures>0</sipSubCountFailures>
</sipSubCountStatistics>
</addressContext>

```

Here is an example wherein to addressContext entity on SBC using RESTCONF API:

```

# curl -H
Authorization:eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiJhZG1pb2IiInVzZXJHcm91cHMlOlsiYWRTaW4iXSwidGVuYW50SWQ0IjIzODQwMDAwMC04Y2YwLTExYmQtYjIzZS0xMGI5NmU0ZWYwMGQ0LCJ1dWlkIjoibmZmMzAyZWQtYzhmNy00ZTg0LTkxZDctYjQ0Y2RhYTg2ODk0IiwiaWF0IjoxNzE5NTYxMDc1LCJleHAiOiJlE5NzV9.EDYN
mdZu9QV080cKQUAdUjxnH0PwPD08mxpdcMKnQqORLl9z2fyhTsx3GbDY0IslXbnyLkt3AJal9QyndWM89pkuxin
EN4E5VysgW0ujXrhGliJzJ3PgL4-
Wm8MSaChUpTWk0f43ADW7PBLpYk23ueyji6Z4yJZRqbZdUHmOgo0r8sMBj4BAHrsP6FjXdQDTwedWlWnoKPmWuv0
mY7k0szqCCHt690fML7_DIXy-
oqPtyqYqtvCbDsv9gyIE9YCvPWq_JUxpMmIzKzE73ggAqzY9tJwwEFl89Mq807ie7vzaSuJBwgyq7WvJvWFumIIq
I-3REoVVsaAf_ZJkIycZg -XPOST -i
https://10.34.146.120/sbxProxy/directIntegrated/restconf/data/
-H 'Content-Type: application/yang-data+xml' --data '<addressContext><name>democontext</
name></addressContext>' --insecure
HTTP/1.1 201
Date: Fri, 28 Jun 2024 07:51:53 GMT
Server: Apache
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, DELETE, PUT, OPTIONS, HEAD

```

```
Last-Modified: Fri, 28 Jun 2024 07:51:53 GMT
Access-Control-Allow-Headers: Content-type, origin, accept, authorization
Access-Control-Allow-Credentials: true
Content-Security-Policy: default-src 'self' blob: data: 'unsafe-eval' 'unsafe-inline'; frame-ancestors 'self';
Location: /restconf/data/sonusAddressContext:addressContext=democontext
Content-Type: text/html;charset=UTF-8
Content-Length: 0
Via: 1.1 cisdCmpRestmicroEMS
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Permitted-Cross-Domain-Policies: master-only
Strict-Transport-Security: max-age=31536000, includeSubDomains, preload
Cache-Control: no-cache, no-store, must-revalidate, private
Pragma: no-cache
```

For more information, refer to [REST API Reference Guide](#).

SOAP API for SBC Core

In this section:

- [API Web Services for SBC](#)
- [Writing an Insight API Client for SBC](#)
 - [Entities Description](#)
- [API Error Handling for SBC](#)
- [SBC Provisioning Operations](#)
 - [SBC SOAP API reference](#)
 - [Provisioning Commands for SBC](#)

Note

Using RAMP to configure the SBC Core using SOAP API is supported only while migrating from EMS to RAMP. Greenfield deployments for RAMP do not support SOAP API, which is deprecated and removed in future releases. Instead, use the REST Proxy to configure SBC Core.

The **Ribbon Application Management Platform (RAMP)** API for SBC is exposed as a collection of web services accessible via SOAP. A Web Service is a programmatic interface that is published for inter-application communication.

- If you have SOAP OSS implementation and require the transition period for the EMS to RAMP migration, this section allows you to migrate to RAMP and build the OSS interface for REST.
- This is a limited feature to support existing EMS SOAP users and not targeting new SOAP deployments.

API Web Services for SBC

Overview

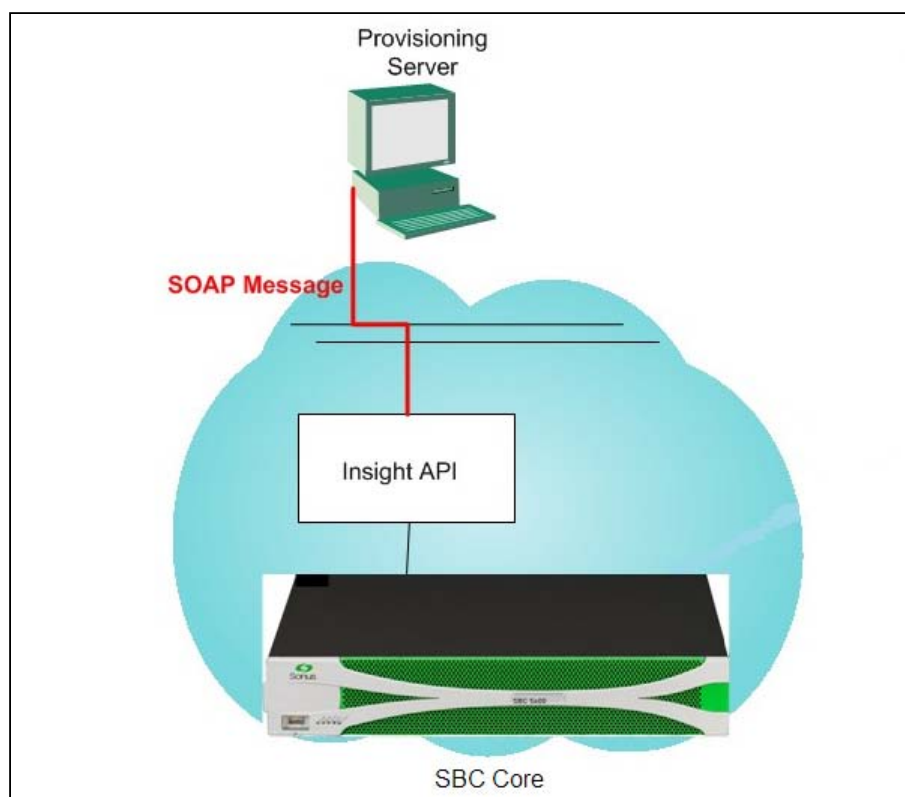
SOAP is a standard for exchanging XML-based messages over a computer network, normally using HTTP. SOAP forms the foundation layer of the web services stack, providing a basic messaging framework that more abstract layers can build upon. SOAP is fundamentally a stateless, one-way message exchange paradigm, but applications can create more complex interaction patterns (for example, request/response, request/multiple responses) by combining such one-way exchanges with features provided by an underlying protocol and/or application-specific information.

SOAP is silent on the semantics of any application-specific data it conveys, as it is on issues such as the routing of SOAP messages, reliable data transfer, firewall traversal, etc. However, SOAP provides the framework by which application-specific information may be conveyed in an extensible manner. Also, SOAP provides a full description of the required actions a SOAP node takes on receiving a SOAP message.

SOAP is an open standard managed by the W3C's XML Protocol Working Group. The following site has more information on the SOAP standard:
"<http://www.w3.org/2000/xp/Group/>".

RAMP API Model for SBC Core

The Ribbon Application Management Platform (RAMP) API set up as illustrated below.



The Insight API for SBC web services are published using WSDL (Web Services Definition Language). WSDL is also an open standard that is managed by the W3C's Web Services Description Working Group. The following site has more information on WSDL: "<http://www.w3.org/2002/ws/desc/>".

Updated and new WSDL files associated with **RAMP** patches are posted on the Ribbon Support Portal along with their associated patch packages.

You need relevant permissions to perform operations on the SBC:

Roles	Operations Supported
Super User (devices.super)	create, update, delete, retrieve, doAction, list
Provisioner (devices.prov)	create, update, delete, retrieve, list
Operator (devices.oper)	retrieve, list
None	None

The SBC APIs are deployed in the background without impacting **RAMP** start time. Once **RAMP** is up, the SBC APIs are deployed within 60 seconds.

To send the SBC API SOAP requests immediately after starting **RAMP**, check whether the SBC APIs are deployed.

Check if the SBC APIs are deployed on **RAMP**:

1. Log on to RAMP CLI.
2. Run the following command as `Insight` user, to check if the `sbcapi.war.deployed` exists on RAMP:

```
ls -lrt /opt/sonus/ems/weblogic/insight/deployments/ |grep sbcapi.war.deployed
```

Ensure that the "SBCAPI:" status is "Deployed" before using the SBC APIs.

Writing an Insight API Client for SBC

In this section:

- [Enabling REST API Using CLI](#)
- [Authentication](#)
- [Client Implementation of JAX-WS](#)
 - [Java Code Generation](#)
 - [Client Example](#)

Note

Beginning with SBC Core release 11.1, REST is transitioned to RESTCONF. RAMP release 26.03 supports RESTCONF by modifying the REST URLs to move to RESTCONF.

Enabling REST API Using CLI

To enable REST API using CLI for admin user:

1. Log on to the SBC CLI.
2. Access CLI in configure mode.
3. Run the following command to enable REST API for admin user:

```
set system admin <YOUR_SYSTEM_NAME> rest state enabled
```

4. Run the following command to enable the machine-to-machine access for admin user:

```
set oam localAuth user admin m2mA
```

5. Commit the changes by running the following command:

```
commit
```

6. To verify the REST API support, use the following command:


```
https://{SBXMGMTIP}/restconf/data/sonusAddressContext:addressContext/
curl -kisu admin:password -s https://{SBX-MGMT-IP}/api/config/addressContext/
```

To verify RESTCONF API support, use the following command:

```
curl -kisu admin:admin -s https://{SBX-MGMT-IP}/restconf/data/
sonusAddressContext:addressContext
```

Authentication

Each operation is authenticated and authorized by checking the user and password elements in the HTTP header. Both the user and password elements are expected in clear text:

```
POST
/sbcapi/v04_02_00/SBCService?wsdl HTTP/1.1
User-Agent: JAX-WS RI 2.2.4-b01
Host:10.54.159.28
Accept: */*
Content-type: text/xml;charset=utf-8
Username: apiuser
Password: apiuser
```

The user and password information in the example above is for illustration purpose only. They must be replaced with a valid Insight user name and password that have been created on RAMP with appropriate operator privileges for the SBC Management. Refer to “Users and Roles.”

Client Implementation of JAX-WS

While the SOAP specification does not mandate a particular language for Web service clients, the following implementation may be helpful.

The Java API for XML Web Services (JAX-WS) is a Java programming language API for working with web services. JAX-WS is one of the Java XML programming APIs. It is part of the Java EE platform.

Wsimport is a tool available in JDK 1.6 and above. This can be found in `JDK_PATH/bin` directory. This tool parses the published `wsdl` file and generates necessary client files to access the webservice.

Java Code Generation

Run the following command to generate the JAVA code:

```
wsimport.exe -keep http://<PROVISIONING_SERVER_IP>/sbcapi/v04_02_00/SBCService?wsdl
```

This generates a number of directories and files with the following structure:

```
com/
-----sonus/
-----ems/
```

```

-----api/
-----sbc/
-----common/
-----v04_02_00/

```

The service directory contains implementation of the Service Definition Interface as defined in the `WSDL` file. This code is used to access the operations defined on the provisioning service. The following operations are defined:

- **Create** - creates entries in the SBC
- **Retrieve** - retrieves details for entries in the SBC
- **PartialRetrieve, RetrieveWithFilterString** – retrieves only specific details for entries in the SBC
- **Update** - updates entries in the SBC
- **Delete** - deletes entries from the SBC
- **doAction** – Performs operations specific to the SBC

Note

The API defines all operations in terms of the following classes:

- SbcKey
- SbcEntity
- SbcOperationKey
- SbcOperationInput
- SbcOperationOutput
- SbcFilter

They are the base classes for all entities. Consequently, the returned values must be cast to the correct type before attempting to access any properties.

The following examples indicates how the returned values are cast using Java.

Example 1:

```

AddressContextKey addressContextKey = new AddressContextKey();
addressContextKey.setName("sampleAddressContext");
zoneKey = new ZoneKey();
zoneKey.setName("sampleZone");
zoneKey.setParentKey(addressContextKey);
Zone zoneRetr = (Zone) api.retrieve(sbcTarget, zoneKey);

```

Example 2:

```

AddressContextKey addressContextKey = new AddressContextKey();
addressContextKey.setName("sampleAddressContext");
zoneKey = new ZoneKey();
zoneKey.setParentKey(addressContextKey);
ZoneListWrapper zonelistRetr = (ZoneListWrapper) api.retrieve(sbcTarget, zoneKey);

```

Example 1 retrieves zone “sampleZone” under address context “sampleAddressContext”.

Example 2 retrieves the list of available zones under address context “sampleAddressContext”. Note that zoneKey object in Example 2 has no name set in it. When no key values are set in a key class, the returning object is a list of zones under that address context.

Client Example

The following code fragment shows how the generated client code can be used to create a zone. The following code assumes that any dependencies have been resolved before this operation is invoked. For example: an address context should exist when a zone is being created under it.

```
package com.sonus.sample;

import java.net.URL;
import java.util.Collections;
import java.util.HashMap;
import java.util.List;
import java.util.Map;

import javax.xml.namespace.QName;
import javax.xml.ws.BindingProvider;
import javax.xml.ws.Service;
import javax.xml.ws.handler.MessageContext;

import com.sonus.ems.api.sbc.v04_02_00.APIAccessException;
import com.sonus.ems.api.sbc.v04_02_00.AddressContext;
import com.sonus.ems.api.sbc.v04_02_00.AddressContextKey;
import com.sonus.ems.api.sbc.v04_02_00.ProvApiException;
import com.sonus.ems.api.sbc.v04_02_00.SBCV040200API;
class ApiExample {
    public static void main(String args[]) {
        SBCV040200API api = null;
        String ipAddress = "10.54.2.80";
        String device = "SampleSBC";
        String username = "apiuser";
        String password = "apiuser";
        String protocol = "http";
        String adCtxTBC = "sampleAddressContext123";
        try {
            String strUrl = protocol + "://" + ipAddress + "/sbcapi/v04_02_00/SBCService?wsdl";
            URL url = new URL(strUrl);
            //1st argument service URI, refer to wsdl
            //2nd argument is service name, refer to wsdl
            QName qname = new QName("http://www.sonus.com/ems/api/sbc/v04_02_00",
"SBC_v04_02_00_APIService");
            Service service = Service.create(url, qname);
            api = service.getPort(SBCV040200API.class);
            Map<String, Object> req_ctx =
((BindingProvider)api).getRequestContext();
            req_ctx.put(BindingProvider.ENDPOINT_ADDRESS_PROPERTY, strUrl);
            Map<String, List<String>> headers = new HashMap<String, List<String>>();
            headers = new HashMap<String, List<String>>();
            headers.put("Username", Collections.singletonList(username));
```

```

        headers.put("Password", Collections.singletonList(password));
        req_ctx = ((BindingProvider)api).getRequestContext();
        req_ctx.put(MessageContext.HTTP_REQUEST_HEADERS, headers);
    }
    catch (javax.xml.ws.WebServiceException e) {
        System.out.println("Exception = " + e.getMessage());
    }
    catch (Exception e) {
        System.out.println("Exception = " + e.getMessage());
    }
    AddressContextKey addressContextKey = new AddressContextKey();
    addressContextKey.setName(adCtxTBC);
    AddressContext addressContext = new AddressContext();
    try {
        api.create(device,addressContextKey, addressContext);
    }
    catch (ProvApiException e) {
        System.out.println("Caughterror. Message: " + e.getMessage());
        System.out.println("Detailed Message: " + ((ProvApiException)
e).getFaultInfo().getMessage());
    } catch (APIAccessException e) {
        System.out.println("Caught error. Message: " + e.getMessage());
        System.out.println("Detailed Message: " + ((APIAccessException)
e).getFaultInfo().getMessage());
    }
    catch (Exception e) {
        System.out.println("Exception = " + e.getMessage());
    }
}
}

```

Entities Description

In this section:

- [SbcEntity](#)
- [SbxInfo](#)
- [SbcKey](#)
- [SbcListWrapper](#)
- [SbcOperationInput](#)
- [SbcOperationKey](#)
- [SbcOperationOutput](#)
- [SbcPayload](#)
- [SbcReadOnlyKey](#)
- [SbcResource](#)
- [SbcFilter](#)
- [SbcSelector](#)
- [SbcSubSelector](#)
- [SbcSubSetFilter](#)
- [SbcUnCreatableKey](#)
- [SbcComplexType](#)

The SBC API entities are heterogeneous. Every entity class is understood by the base classes it extends or implements. All the java client classes generated extend or implement one of the following classes.

SbcEntity

Top level base class which represents an entity. All the entities extend SbcEntity.

SbxInfo

A class which retrieves the SBC Core device details.

SbcKey

A common base class which uniquely identifies an entity. All the entity key classes extend the SbcKey.

SbcListWrapper

A common base class which represents an entity wrapper response. When the Sbc response is a collection of similar entities, it is retrieved as an SbcListWrapper. All the entities wrapper classes extend SbcListWrapper. The user need not set any key values in the SbcKey type object for retrieving an SbcListWrapper type object.

```
SbcSubSetFilter sbcSubSetFilter = new SbcSubSetFilter();
sbcSubSetFilter.setOffset(2); sbcSubSetFilter.setLimit(5);
dnsGroupKey = new DnsGroupKey();
dnsGroupKey.setParentKey(addressContextKey);
dnsGroupWrapper = (DnsGroupListWrapper) api.partialRetrieve(sbcTarget, dnsGroupKey,
sbcSubSetFilter);
```

The above example retrieves five dnsGroup entries starting from entry two (the first entry is 0).

SbcOperationInput

Represents the input for an SBC action.

SbcOperationKey

Key representation of an SBC action. You must set the parent relationship for this entity through SbcOperationKey.

SbcOperationOutput

Represents the output for an SBC action.

SbcPayload

Represents payload for entities, listWrappers and SBC actions. All the retrieve variant methods (retrieve, partialRetrieve, retrieveWithFilterString) return an object of SbcPayload type.

SbcReadOnlyKey

Represents ready only entities. You cannot create, update, or delete ready only entities . Only retrieve operation is supported. Other operations show a SOAP fault with ERR_READONLY_KEY code.

SbcResource

Represents a top level entity. The root level entities are referenced through SbcResource.

SbcFilter

A filter class to specify if the response retrieved from SBC is deep or shallow. It is deep by default. Use the shallow flag in conjunction with parameters in SbcSelector and SbcSubSetFilter.

```
SbcFilter sbcFilter = new SbcFilter();
sbcFilter.setShallow(true);
SBCV040200API sbcV040200API = new SBCV040200API();
sbcV040200API.partialRetrieve(sbcName, sbcKey, sbcFilter);
```

SbcSelector

A filter class to select only a subset of nodes and/or attributes' values when performing a retrieve operation. SbcSelector restricts retrieve response only to the set of attributes, entities user is interested in. SbcSelector can take any number of attributes and entities.

```
String simpleNode = "cmds";
SbcSelector sbcSelector = new SbcSelector();
sbcSelector.getNodeNames().add(simpleNode);
SbcSubSelector dnsGroupSubSelector = new SbcSubSelector();
String entityName = "dnsGroup";
String subSelectorSimpleNode1 = "name";
String subSelectorSimpleNode2 = "mgmtInterface";
dnsGroupSubSelector.setEntity(entityName);
SbcSelector sbcSelectorChild = new SbcSelector();
sbcSelectorChild.getNodeNames().add(subSelectorSimpleNode1);
sbcSelectorChild.getNodeNames().add(subSelectorSimpleNode2);
dnsGroupSubSelector.setSelector(sbcSelectorChild);
sbcSelector.getSubSelectors().add(dnsGroupSubSelector);
sbcSelector.setShallow(true);
addCtxRetr = (AddressContext) api.partialRetrieve(sbcTarget, addressContextKey,
sbcSelector);
```

The above example retrieves cmds ,dnsGroup/name ,dnsGroup/mgmtInterface

SbcSubSelector

A SbcSubSelector object holds the entity name and SbcSelector objects again. This class is used for setting values for SbcSelector.

```
SbcSubSelector dnsGroupSubSelector = new SbcSubSelector();
String entityName = "dnsGroup";
String subSelectorSimpleNode1 = "name";
String subSelectorSimpleNode2 = "mgmtInterface";
dnsGroupSubSelector.setEntity(entityName);
SbcSelector sbcSelectorChild = new SbcSelector();
```

```
sbcSelectorChild.getNodeNames().add(subSelectorSimpleNode1);
sbcSelectorChild.getNodeNames().add(subSelectorSimpleNode2);
dnsGroupSubSelector.setSelector(sbcSelectorChild);
```

SbcSubSetFilter

A filter class to select only a subset of nodes specifying limit and offset when performing a retrieve operation. SbcSubSetFilter is a sub-class of SbcFilter, the user can also set or unset shallow flag.

This filter is valid only for a collection of similar entities. You must not set any key values in the SbcKey type object to make sure a wrapper class object is retrieved.

```
SbcSubSetFilter sbcSubSetFilter = new SbcSubSetFilter();
sbcSubSetFilter.setOffset(2);
sbcSubSetFilter.setLimit(5);
DnsGroup dnsGroupKey = new DnsGroupKey();
dnsGroupKey.setParentKey(addressContextKey);
DnsGroupListWrapper dnsGroupWrapper = (DnsGroupListWrapper)
api.partialRetrieve(sbcTarget, dnsGroupKey, sbcSubSetFilter);
```

The above example retrieves five DnsGroup entries starting from entry two (the first entry is 0).

SbcUnCreatableKey

This class represents the entities that you cannot create or delete. The entities already exist. User can only update or retrieve the entity.

SbcComplexType

The SbcComplexTypes are introduced to help the user in creating the bits/union types. All the Bits, Union classes implement this interface.

The client has two fields for each bits/union type attribute. Bits and Union types are represented by classes whose names end with Bits and Union respectively.

When sending the request, the client sets the field with suffix Bits/Union.

On the receiving side, the decoding to the actual SbcComplexType is not implemented, instead look at the String type.

Bits Usage

Bits type classes contain a set of boolean variables. All the attributes that set for an entity have their boolean flag set to true.

```
SonusTransportProtocolsAllowedTypeBits sonusTransportProtocolsAllowedTypeBits = new
SonusTransportProtocolsAllowedTypeBits();
sonusTransportProtocolsAllowedTypeBits.setSipSctp(true);
sonusTransportProtocolsAllowedTypeBits.setSipTlsTcp(true);
sipSigPort = new SipSigPort();
```

```
sipSigPort.setTransportProtocolsAllowedBits(sonusTransportProtocolsAllowedTypeBits); -
(1)
```

Note

(1) - Additionally, the user can also set the bits value in String format. In case of multiple bits, each bit String should be separated by space. [sipSigPort.setTransportProtocolsAllowed("sipsctp siptlstcp");

Union Usage

Union type classes contain variables of different data types. This type is analogous to unions in C language. The user has to set only one variable in a given union type. If multiple variables are set, only the first variable encountered will be considered and rest of them will be discarded.

```
SonusCacCallLimitTypeUnion union = new SonusCacCallLimitTypeUnion();
union.setSonusCacLimitTypeUnlimited("unlimited"); -(2)
cac.setCallLimitUnion(union);
```

Note

(2) – User can also perform union.setSonusCacLimitTypeVal(123) for the same union instead.

API Error Handling for SBC

In this section:

- [API Provisioning Errors Summary](#)
 - `<faultcode>`
 - `<faultstring>`
 - `<detail>`
 - [ProvApiException](#)
 - [ApiAccessException](#)
- [API Provisioning Error Codes](#)

API Provisioning Errors Summary

Provisioning errors are generated by the SBC or the provisioning server. The API returns these errors encapsulated as SOAP faults.

The structure of the SOAP fault (contained within the SOAP body) is as follows:

```
<S:Fault>
  <faultcode>S:Server</faultcode>
```



```

    <faultstring>ERROR_CODE</faultstring>
    <detail>
      <ns3:ProvApiException>
        <message>ERROR_MESSAGE</message>
      </ns3:ProvApiException>
    </detail>
  </S:Fault>

```

<faultcode>

The faultcode element contains an error indication that is generated by the SOAP engine.

The value S:Server indicates that the error is generated by the provisioning server.

<faultstring>

The fault string contains one of the error codes.

<detail>

The detail element contains a reference to one of three types of errors that are defined in the API:

```

com.sonus.ems.api.sbc.v04_02_00.ProvApiException
com.sonus.ems.api.sbc.v04_02_00.ApiAccessException

```

The message string inside the detail element gives more information about the fault.

ProvApiException

This is the generic exception that can be thrown by the API. It contains an error code and a message.

The following is the extract from WSDL file that defines the structure of a `ProvApiException`:

```

<message name="ProvApiException">
  <part name="fault" element="tns:ProvApiException"/>
</message>

```

The following is a SOAP response containing a `ProvApiException`:

```

<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <S:Body>
    <S:Fault xmlns:ns3="http://www.w3.org/2003/05/soap-envelope" xmlns="">
      <faultcode>S:Server</faultcode>
      <faultstring>ERR_INVALID_KEY</faultstring>
      <detail>
        <ns3:ProvApiException
          xmlns:ns3="http://www.sonus.com/ems/api/sbc/v04_02_00"
          xmlns:ns2="v04_02_00.sbc.api.ems.sonus.com">
          <message>Invalid key

```

```

        com.sonus.ems.api.sbc.v04_02_00.global.callrouting.Rout
        eKey callTypeBits key is null--</message>
    </ns3:ProvApiException>
</detail>
</S:Fault>
</S:Body>
</S:Envelope>

```

ApiAccessException

This is thrown if :

1. The user tries to access the api methods with improper username and/or password.
2. The user account used for the provisioning action does not have sufficient access privileges to perform the operation.

Each SBC operation requires the user to possess a certain level of Authorization. The authorization level and operations permitted are listed in the following table:

User roles and the operations supported

Roles	Operations Supported
Super User (devices.super)	create, update, delete, retrieve, doAction, list
Provisioner (devices.prov)	create, update, delete, retrieve, list
Operator (devices.oper)	retrieve, list
None	None

The following is the extract from WSDL file that defines the structure of a `ApiAccessException` :

```

<message name="APIAccessException">
    <part name="fault" element="tns:ApiAccessException"/>
</message>

```

The following is a SOAP response containing a `ApiAccessException` that occurred when an invalid username/password is supplied:

```

<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <S:Body>
        <S:Fault
            xmlns:ns3="http://www.w3.org/2003/05/soap-envelope" xmlns="">
            <faultcode>S:Server</faultcode>
            <faultstring>ERR_AUTHENTICATION_FAIL</faultstring>
            <detail>

```

```

        <ns3:ApiAccessException
xmlns:ns3="http://www.sonus.com/ems/api/sbc/v04_02_00"
xmlns:ns2="v04_02_00.sbc.api.ems.sonus.com">
            <message>Invalid user and/or password</message>
        </ns3:ApiAccessException>
    </detail>
</S:Fault>
</S:Body>
</S:Envelope>

```

The following is a SOAP response containing a `ApiAccessException` that occurred when user with insufficient access privileges is supplied:

```

<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <S:Body>
        <S:Fault
xmlns:ns3="http://www.w3.org/2003/05/soap-envelope" xmlns="">
            <faultcode>S:Server</faultcode>
            <faultstring>ERR_AUTHORIZATION_FAIL</faultstring>
            <detail>
                <ns3:ApiAccessException
xmlns:ns3="http://www.sonus.com/ems/api/sbc/v04_02_00"
xmlns:ns2="v04_02_00.sbc.api.ems.sonus.com">
                    <message>You are not authorized to perform this
operation</message>
                </ns3:ApiAccessException>
            </detail>
        </S:Fault>
    </S:Body>
</S:Envelope>

```

API Provisioning Error Codes

Provisioning Error Codes

Error Code	Meaning
ERR_INVALID_VAL	There is an invalid value in the payload. This usually occurs for create or update operation.
ERR_SBC_AUTHENTICATION	The username [Agent Login] and password [Agent Password] provided for SBC during registration of the device on RAMP are wrong
ERR_SBC_AUTHORIZATION	The username [Agent Login] and password [Agent Password] provided for SBC during registration of the device on RAMP do not have sufficient privilege to perform the operation
ERR_REC_NOT_FOUND	The record doesn't exist usually comes when the user tries to retrieve a non-existent entity from the SBC
ERR_REC_EXISTS	The record already exists usually comes when a user tries to create a resource which is already existing.
ERR_CONFIGURABLE_KEY	Trying to create or delete a Presence Key (a special key) in SBC. These type of keys can only be read or updated, but cannot be created or deleted.
ERR_READONLY_KEY	Trying to perform a non-read operation (create/update/delete) on a read-only key
ERR_UNKNOWN_DEVICE	Executing an API operation on an unregistered SBC on the given RAMP.
ERR_INVALID_KEY	The key object created by the client is invalid.
ERR_AUTHORIZATION_FAIL	The username and password used for invoking the API operation do not have sufficient authorization level to perform that operation.
ERR_AUTHENTICATION_FAIL	The username and password used for invoking the API operation are wrong.
ERR_API_INTERNAL	An error is caught by the RAMP server during the web service call.

SBC Provisioning Operations

In this section:

- [SBC SOAP API reference](#)
- [Provisioning Commands for SBC](#)
 - [Operation: create for SBC](#)
 - [Operation: delete for SBC](#)
 - [Operation: doAction for SBC](#)
 - [Operation: getSbcList](#)
 - [Operation: partialRetrieve for SBC](#)
 - [Operation: retrieve for SBC](#)
 - [Operation: retrieveWithFilterString for SBC](#)
 - [Operation: update for SBC](#)

Each entity defined in the WSDL file extends from one of the following classes:

- **SbckKey**: A common base class which represents an entity key. All the entity key classes extend the SbckKey. the object of this class contains the key values for the entity to be created and also specifies the hierarchy to create the given entity.
- **SbcEntity**: A common base class which represents an entity. All the entities extending the SbcEntity. Input for create and update operations are an object of SbcEntity type.
- **SbcOperationKey**: Key representation of an SBC action. Set the parent relationship for this entity through SbcOperationKey.
- **SbcOperationInput**: The input for an SBC action.
- **SbcOperationOutput**: The output of an SBC action.
- **SbcFilter**: This filter class specifies if the received response from the SBC is deep or shallow. By default, SbcFilter is set to "deep". Use the "shallow" flag in conjunction with SbcSelector and SbcSubSetFilter settings.
- **SbcSelector**: This filter class selects only a subset of nodes and/or attribute values when performing a retrieve operation. Based on the SbcSelector filter settings, the retrieve response is restricted to only to the set of attributes, entities of interest. The SbcSelector field allows configuring any number of attributes and entities.
- **SbcSubSelector**: This class holds the entity name and SbcSelector objects to set the values for SbcSelector.
- **SbcSubSetFilter**: This filter class selects only a subset of nodes specifying the limit and offset when performing a retrieve operation. The SbcSubSetFilter is a sub-class of SbcFilter, from which you can set or unset the "shallow" flag.

Each operation/method is documented with respect to the aforementioned classes.

Each entity has a different set of required properties, and not all entities support each operation/method. In addition, it is not necessary to supply values for every property of each entity.

For each operation, key values are only populated in SbckKey sub-classes. Any key values set in the SbcEntity sub-classes (pay load) are ignored.

SBC SOAP API reference

The SBC SOAP API Javadoc reference (`sbc_api_doc_vxx_yy_zz.zip`) is available on Ribbon Support Portal. Download the API reference file from Ribbon Support Portal to your local server or system.

Note

"xx_yy_zz" is the respective SBC version supported. For example, if the SBC version supported is 04.02.00 then, the Javadoc reference file will be `sbc_api_doc_v04_02_00.zip`.

Execute the following steps to download the files from Ribbon Support Portal.

1. Log in to the Ribbon support portal.
2. In Secure Customer Login, enter your **Username** and **Password**. The Ribbon Support Portal displays.
3. From the Ribbon Support Portal, click **SOFTWARE DOWNLOADS** tab. The Software Downloads screen displays.
4. Download the Javadoc file (`sbc_api_doc_vxx_yy_zz.zip`) on to your local system or local server.
5. Unzip to extract all the files.
6. Click on `index.html` file to get all the information about the various entities and operations.

Provisioning Commands for SBC

In this section:

- [Operation: create for SBC](#)
- [Operation: delete for SBC](#)
- [Operation: doAction for SBC](#)
- [Operation: getSbcList](#)
- [Operation: partialRetrieve for SBC](#)
- [Operation: retrieve for SBC](#)
- [Operation: retrieveWithFilterString for SBC](#)
- [Operation: update for SBC](#)

Operation: create for SBC

Creates a new entry in the SBC Server 'sbcName'.

Format

```
void create (String sbcName,SbcKey target, SbcEntity payload)
```

where:

- sbcName is the name of the SBC registered on the **Ribbon Application Management Platform (RAMP)**.
- target object contains the key values for the entity to be create. It also specifies under which hierarchy to create the given entity.
- payload contains the non-key values (both mandatory and optional) values for the entity to be create.

The following sample code creates a DnsGroup “sampleDnsGroup” under AddressContext “sampleAddressContext” to help you understand how to create an entity at a given level.

```
addressContextKey = new AddressContextKey();
addressContextKey.setName("sampleAddressContext");
dnsGroupKey = new DnsGroupKey();
dnsGroupKey.setName("sampleDnsGroup");
dnsGroupKey.setParentKey(addressContextKey);
DnsGroup dnsGroup = new DnsGroup();
dnsGroup.setType(SonusInterfaceType.MGMT);
api.create(sbcTarget, dnsGroupKey, dnsGroup);
```

This code assumes the Address Context “sampleAddressContext” exists and creates the Dns Group “sampleDnsGroup” under it.

The steps involved in the create operation are:

1. Creates AddressContextKey object and add key values to it (name in this case).
2. Creates DnsGroupKey object and add the key values to it (name in this case).
3. DnsGroupKey object specifies Address Context “sampleAddressContext” as its parent using setParentKey method.
4. Creates payload in DnsGroup object, and add non-key values to it (type in this case).
5. Passes DnsGroupKey and DnsGroup objects as arguments to create operation.

Even though there is no payload associated with a create operation in a given scenario, you must create a new object and pass it to the operation because a null payload is a BP 1.1 R2211 violation.

Operation: delete for SBC

Deletes an existing entry in the SBC Server 'sbcName'.

Format

```
void delete(String sbcName,SbcKey target)
```

where:

- sbcName is the name of the SBC registered on the Ribbon Application Management Platform (RAMP).
- target object contains the key values for the entity to create. It also specifies under which hierarchy to create the given entity.

Here is a sample code to understand how an entity should be deleted at a given level.

The following code deletes a DnsGroup “sampleDnsGroup” under AddressContext “sampleAddressContext”.

```
addressContextKey = new AddressContextKey();
```

```
addressContextKey.setName("sampleAddressContext");
dnsGroupKey = new DnsGroupKey();
dnsGroupKey.setName("sampleDnsGroup");
dnsGroupKey.setParentKey(addressContextKey);
api.delete(sbcTarget,dnsGroupKey);
```

This code assumes the Address Context “sampleAddressContext” and Dns Group “sampleDnsGroup” objects exist.

Below are the steps involved in the delete operation:

1. Creates AddressContextKey object and adds key values to it ("name" in this case).
2. Creates DnsGroupKey object and adds the key values to it ("name" in this case).
3. DnsGroupKey object specifies Address Context “sampleAddressContext” as its parent using setParentKey method.
4. Passes DnsGroupKey object as an argument to delete operation.

Operation: doAction for SBC

Performs actions on the SBC Server 'sbcName'.

Format

```
SbcOperationOutput doAction (String sbcName, SbcOperationKey target, SbcOperationInput
operationInput)
```

where:

- sbcName is the name of the SBC registered on the Ribbon Application Management Platform (RAMP).
- target object specifies under what hierarchy the given action should be performed.
- operationInput contains the input parameter values for the action to be performed.

Here is a sample code to understand how an operation should be performed at a given level.

```
addressContextKey = new AddressContextKey();
addressContextKey.setName("sampleAddressContext");
addressContext = new AddressContext();
api.create(sbcTarget, addressContextKey, addressContext);
SipRegistrationDeleteByIpKey sipRegistrationDeleteByIpKey = new
SipRegistrationDeleteByIpKey();
sipRegistrationDeleteByIpKey.setParentKey(addressContextKey);
SipRegistrationDeleteByIp sipRegistrationDeleteByIp = new SipRegistrationDeleteByIp();
sipRegistrationDeleteByIp.setIpAddress("1.2.3.4");
Output op = (Output) api.doAction(sbcTarget, sipRegistrationDeleteByIpKey,
sipRegistrationDeleteByIp);
```

The above code assumes the Address Context “sampleAddressContext” has already been created and SipRegistrationDeleteByIpKey action is being performed under it.

Below are the steps involved in the doAction operation:

1. AddressContextKey object is created and key values are set in it ("name" in this case).
2. SipRegistrationDeleteByIpKey object is created.
3. SipRegistrationDeleteByIpKey object specifies Address Context "sampleAddressContext" as its parent using setParentKey method.
4. sipRegistrationDeleteByIp object (payload is created) with operation input parameters set in it (ipAddress in this case).
5. sipRegistrationDeleteByIpKey and sipRegistrationDeleteByIp objects are passed as arguments to the doAction operation.

The class to represent the output of an action class can be found in the corresponding action package suffixed with Output. If the action specific output class not found then use the common SbcOperationOutput class.

Operation: getSbcList

To retrieve the list of SBC Core nodes registered and online on the Ribbon Application Management Platform (RAMP):

HTTP Method: POST

Endpoint to hit:

```
https://<EMS_IP>/sbcap/api/SBC_LIST_APIService
```

Request Body:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:sbc="http://www.sonus.com/ems/api/sbc/sbcList">
  <soapenv:Header/>
  <soapenv:Body>
    <sbc:getSbcList>
      <sbcName></sbcName>
    </sbc:getSbcList>
  </soapenv:Body>
</soapenv:Envelope>
```

Example response/output:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/>
<soap:Body>
  <ns1:getSbcListResponse xmlns:ns1="http://www.sonus.com/ems/api/sbc/sbcList">
    <SbcList>
```

```

    <item>
      <ip>10.54.41.40</ip>
      <lastChangeTime>1577998634989</lastChangeTime>
      <lastDiscoveryStatus>0</lastDiscoveryStatus>
      <name>sbcl</name>
      <nodeId>10023</nodeId>
      <snmpVersion>1</snmpVersion>
    </item>
    <item>
      <ip>10.54.41.41</ip>
      <lastChangeTime>1577998188657</lastChangeTime>
      <lastDiscoveryStatus>0</lastDiscoveryStatus>
      <name>sbcl</name>
      <nodeId>10030</nodeId>
      <snmpVersion>1</snmpVersion>
    </item>
  </SbcList>
</ns1:getSbcListResponse>
</soap:Body>
</soap:Envelope>

```

To retrieve the details of an SBC Core node registered and online on RAMP:

You can specify the name of the SBC Core node. No other parameters are supported.

HTTP Method: POST

Endpoint to hit:

https://<EMS_IP>/sbccapi/SBC_LIST_APIService

Request Body:

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:sbc="http://www.sonus.com/ems/api/sbc/sbcList">
  <soapenv:Header/>
  <soapenv:Body>
    <sbc:getSbcList>
      <sbcName>sbcl</sbcName>
    </sbc:getSbcList>
  </soapenv:Body>
</soapenv:Envelope>

```

where:

- sbcl is the name of the SBC Core node registered on RAMP.
- APIAccessException is the error code for authentication issues with SOAP client credentials.
- ProvApiException is the error code for provisioning issues in the SOAP request.

Example response/output:

```

<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"/>
<soap:Body>
  <ns1:getSbcListResponse xmlns:ns1="http://www.sonus.com/ems/api/sbc/sbcList">
    <SbcList>
      <item>
        <ip>10.54.41.40</ip>
        <lastChangeTime>1577998634989</lastChangeTime>
        <lastDiscoveryStatus>0</lastDiscoveryStatus>
        <name>sbc</name>
        <nodeId>10023</nodeId>
        <snmpVersion>1</snmpVersion>
      </item>
    </SbcList>
  </ns1:getSbcListResponse>
</soap:Body>
</soap:Envelope>

```

Operation: partialRetrieve for SBC

Retrieves a subset of existing entries based on a filter in the SBC Server 'sbcName'.

Format

```
void partialRetrieve(String sbcName, SbcKey target, SbcFilter filter)
```

where:

- sbcName is the name of the SBC registered on the Ribbon Application Management Platform (RAMP).
- target object contains the key values for the entity to be created. It also specifies under what hierarchy the given entity should be created.
- filter object holds the pattern with which only a subset of the whole retrieve response can be requested
- SbcFilter is base class of SbcSelector and SbcSubSetFilter. The retrieve method can accept one of the three filter classes' object.

The below table explains each of the filters and its functionality.

Filter and its functionalities

Filter	Functionality
SbcFilter	Specify if all the (or) only vital information of the entity and its children should be retrieved
SbcSelector	Restrict retrieve response only to the set of attributes, entities user is interested in.
SbcSubSetFilter	Restrict retrieve response only to a subset of entities specified by limit and offset.

Let us assume the address context “sampleAddressContext” is created and 1000 dns groups (sampleDnsGroup0 to sampleDnsGroup4) are created under “sampleAddressContext”. This assumption will be valid for the section [Operation: retrieveWithFilterString for SBC](#).

```
addressContextKey = new AddressContextKey();
addressContextKey.setName("sampleAddressContext");
dnsGroup = new DnsGroup();
dnsGroup.setType(SonusInterfaceType.NONE);
dnsGroup.setMgmtInterface("mgmtGroup");
for (int i = 0; i < 5; i++)
{
    dnsGroupKey = new DnsGroupKey();
    dnsGroupKey.setName("sampleDnsGroup"+i);
    dnsGroupKey.setParentKey(addressContextKey);
    -api.create(sbcTarget, dnsGroupKey, dnsGroup);
}
```

SbcFilter

SbcFilter contains a boolean flag shallow which specifies if the response should be deep or shallow.

If the shallow flag is unset, the retrieve method responds with all the information of the entity and its children. If the shallow flag is set, only vital information of the entity and its children is retrieved.

By default, the retrieve’s shallow flag is set to false. In other words, when retrieve method is called, all the information of the entity and its children is retrieved by default. If the user wants only vital information in retrieve’s response, SbcFilter object should be used and partialRetrieve method should be called.

Here is a sample code to understand how an entity should be retrieved with SbcFilter object at a given level.

The below code retrieves “sampleAddressContext”, the dns group information in the response is restricted to dns group names. Since shallow is set, the type and management interface are null.

```
SbcFilter sbcFilter = new SbcFilter();
sbcFilter.setShallow(true);
AddressContext addCtxRetr = (AddressContext)api.partialRetrieve(sbcTarget,
addressContextKey,sbcFilter);
```

Below are the steps involved in the above retrieve operation:

1. SbcFilter object is created and shallow flag is set to true.
2. partialRetrieve method is called with sbcName, addressContextKey and sbcFilter objects as arguments.

SbcSelector

SbcSelector is a sub-class of SbcFilter. The functionality of SbcSelector is to restrict retrieve response only to the set of attributes, entities user is interested in. This filter can take any number of attributes and entities.

SbcSelector contains the following variables:

- An object "selector" which accepts a SbcSelector object. The "selector" object represents the children of this child entity (which is again SbcSelector). Hence, the object can be extended to any level of children.

SbcSubSelector class represents a child entity. This class contains the following variables:

1. A String "entity" which represents name of the child entity.
2. A list "subSelectors" which accepts SbcSubSelector objects. The list "subSelectors" represents the children of this child entity (which are entities again). Hence, the list can be extended to any level of children.

Since SbcSelector is a sub-class of SbcFilter, the user can also set or unset shallow flag.

Here is a sample code to understand how an entity should be retrieved with SbcSelector object at a given level.

In the following example setting "select=cmds;dnsGroup(name;mgmtInterface)" select only cmds and name,mgmtInterface of dnsGroup from the result

```
String simpleNode = "cmds";
SbcSelector sbcSelector = new SbcSelector();
sbcSelector.getNodeNames().add(simpleNode);
SbcSubSelector dnsGroupSubSelector = new SbcSubSelector();
String entityName = "dnsGroup";
String subSelectorSimpleNode1 = "name";
String subSelectorSimpleNode2 = "mgmtInterface";
dnsGroupSubSelector.setEntity(entityName);
SbcSelector sbcSelectorChild = new SbcSelector();
sbcSelectorChild.getNodeNames().add(subSelectorSimpleNode1);
sbcSelectorChild.getNodeNames().add(subSelectorSimpleNode2);
dnsGroupSubSelector.setSelector(sbcSelectorChild);
sbcSelector.getSubSelectors().add(dnsGroupSubSelector);
sbcSelector.setShallow(true);
addCtxRetr = (AddressContext) api.partialRetrieve(sbcTarget, addressContextKey,
sbcSelector);
```

Below are the steps involved in the above retrieve operation:

1. SbcSelector object "sbcSelector" is created.
2. A String "cmds" is added to SbcSelector's "nodeNames" list. This represents that the user wants to retrieve cmds under address context.
3. A SbcSubSelector dnsGroupSubSelector is created. It is named "dnsGroup" by setting the entity String.
4. A child SbcSelector "sbcSelectorChild" is created and two attributes of dns group, namely "name" and "management interface" are added to "nodeNames" of "sbcSelectorChild".
5. The "sbcSelectorChild" is set to dnsGroupSubSelector's "selector" object. This represents that user want to retrieve name & mgmtInterface under "dnsGroup".
6. The dnsGroupSubSelector is added to "sbcSelector" object.

SbcSubSetFilter

SbcSubSetFilter is a sub-class of SbcFilter. The functionality of SbcSubSetFilter is to restrict retrieve response only to a subset of entities specified by limit and offset.

SbcSubSetFilter contains limit and offset integer variables to specify limit and offset restriction respectively. Since, limit and offset can be applied only on a list of entities. This filter should be applied only when a user expects a wrapper response.

Since SbcSubSetFilter is a sub-class of SbcFilter, the user can also set or unset shallow flag.

Here is a sample code to understand how an entity should be retrieved with SbcSubSetFilter object at a given level.

In the following example setting offset=2 and Limit=2, retrieves 2 DnsGroup entries starting from entry 2(the index of first entry is 0).

```
SbcSubSetFilter sbcSubSetFilter = new SbcSubSetFilter();
sbcSubSetFilter.setOffset(2);
sbcSubSetFilter.setLimit(2);
dnsGroupKey = new DnsGroupKey();
dnsGroupKey.setParentKey(addressContextKey);
dnsGroupWrapper = (DnsGroupListWrapper) api.partialRetrieve(sbcTarget,
dnsGroupKey, sbcSubSetFilter);
```

Below are the steps involved in the above retrieve operation:

1. SbcSubSetFilter object is created; Limit and offset values are set.
2. DnsGroup payload object is created, no variables should be set (to make sure Wrapper response is retrieved).

Operation: retrieve for SBC

Retrieves an existing entry in the SBC Server 'sbcName'.

Format

```
void retrieve(String sbcName, SbcKey target)
```

where:

- sbcName is the name of the SBC registered on the Ribbon Application Management Platform (RAMP).
- target object contains the key values for the entity to be created. It also specifies under what hierarchy the given entity should be created.

Here is a sample code to understand how an entity should be retrieved at a given level.

Below code retrieves a DnsGroup “sampleDnsGroup” under AddressContext “sampleAddressContext”.

```
addressContextKey = new AddressContextKey();
```

```
addressContextKey.setName("sampleAddressContext");
dnsGroupKey = new DnsGroupKey();
dnsGroupKey.setName("sampleDnsGroup");
dnsGroupKey.setParentKey(addressContextKey);
api.retrieve(sbcTarget, dnsGroupKey);
```

The above code assumes the Address Context “sampleAddressContext” and Dns Group “sampleDnsGroup” have already been created.

Below are the steps involved in the retrieve operation:

1. AddressContextKey object is created and key values are set in it ("name" in this case).
2. DnsGroupKey object is created and the key values are set in it ("name" in this case).
3. DnsGroupKey object specifies Address Context “sampleAddressContext” as its parent using setParentKey method.
4. DnsGroupKey object is passed as an argument to retrieve operation.

Operation: retrieveWithFilterString for SBC

This method is same as partialRetrieve method, but takes filter argument in String format. This method comes in handy if the user wants to create a filter directly in String format than creating a filter object.

Format

```
void retrieveWithFilterString (String sbcName, SbcKey target, String filter)
```

where:

- sbcName is the name of the SBC registered on on the Ribbon Application Management Platform (RAMP).
- target object contains the key values for the entity to be created. It also specifies under what hierarchy the given entity should be created.
- filter String holds the pattern with which only a subset of the whole retrieve response can be requested.

```
Object response = (Object) api.retrieveWithFilterString(sbcTarget, dnsGroupKey,
filterString);
```

The filterString argument in the above method call can either be SbcSelector or SbcSubSetFilter in String format.

FILTER CLASS	FILTER STRING	EXPLANATION
SbcSelector	"fields=cmds;dnsGroup(name;mgmtInterface)"	Select only cmds and name,mgmtInterface of dnsGroup from the result
SbcSubSetFilter	"limit=2&offset=2"	Select only subset of the result, limit the size by 2 and offset by 2

Operation: update for SBC

Updates an existing entry in the SBC Server 'sbcName'.

Format

```
void update(String sbcName, SbcKey target, SbcEntity payload)
```

where:

- sbcName is the name of the SBC registered on the Ribbon Application Management Platform (RAMP).
- target object contains the key values for the entity to be updated. It also specifies under what hierarchy the given entity should be created.
- payload contains the non-key values (both mandatory and optional) values for the entity to be created.

Key values cannot be updated and any key values set in the payload will be ignored.

Here is a sample code to understand how an entity should be updated at a given level.

Below code updates the type of DnsGroup "sampleDnsGroup" to MGMT under AddressContext "sampleAddressContext".

```
addressContextKey = new AddressContextKey();
addressContextKey.setName("sampleAddressContext");
dnsGroupKey = new DnsGroupKey();
dnsGroupKey.setName("sampleDnsGroup");
dnsGroupKey.setParentKey(addressContextKey);
DnsGroup dnsGroup = new DnsGroup();
dnsGroup.setType(SonusInterfaceType.MGMT);
api.update(sbcTarget, dnsGroupKey, dnsGroup);
```

The above code assumes the Address Context "sampleAddressContext" and Dns Group "sampleDnsGroup" have already been created.

Below are the steps involved in the update operation:

1. AddressContextKey object is created and key values are set in it (name in this case).
2. DnsGroupKey object is created and the key values are set in it (name in this case).
3. DnsGroupKey object specifies Address Context "sampleAddressContext" as its parent using setParentKey method.
4. DnsGroup object (payload is created) with non-key values set in it (type in this case).
5. DnsGroupKey and DnsGroup objects are passed as arguments to update operation.

SOAP API for PSX

Ribbon Application Management Platform (RAMP) APIs for PSX are a collection of web services accessible via Simple Object Access Protocol (SOAP). A web service is a programmatic interface that is published for inter-application communication.

The PSX API uses Web Services Definition Language (WSDL) to publish its web services. Using a SOAP API client, the xml request is sent to RAMP, which redirects the request on to the PSX using the Policy Information Provisioning Engine (PIPE).

The WSDL files are available on RAMP at the following location: /opt/sonus/ems/sdk/psxapi/axis_1.2.1

The WSDL can also be accessed through the following URL:

`https://<RAMP IP address>/emsapi/services/PSXAPI/r<PSX version>?wsdl`

The following is an example:

`https://10.52.23.13/emsapi/services/PSXAPI/r12_02_00?wsdl`

When you access the WSDL file using the URL, the location listed within the "wsdlsoap:address location" tag is incorrect.

The following is an example:

```
"http://127.0.0.1:8080/emsapi/services/PSXAPI/PSXAPI/r12_02_00"
```

The corrected location is:

```
"http://127.0.0.1:8080/emsapi/services/PSXAPI/r12_02_00"
```

For more information on the PSX API, refer to [PSX API Programmer Reference](#).

For trace and debugging purpose, use the following log files available at `/opt/sonus/ems/weblogic/sonusEms/logs/sys:`

- `emsapi_debug_log`
- `emsapi_prov_log`
- `ems_trace_log`

PSX CLI Through RAMP

The Ribbon Application Management Platform (RAMP) CLI supports issuing PSX commands.

Perform SSH through port 8122 to enter PSX commands from the RAMP CLI.

Note

The idle timeout interval for a CLI session is set to 30 minutes.

Prerequisites

- You must have **Super User** [privileges](#) for **CLI** under **Core Resources**.
- The PSX device is registered on RAMP.
- The SSH client supports at least one of the following Ciphers/Kex/MACs:
- Ciphers:

```
aes-192ctr
```

- Kex:

```
ecdh_sha2_nistp384
ecdh_sha2_nistp521
diffie_hellman_group14_sha1
diffie_hellman_group14_sha256
```

- MACS:

```
hmacsha256
hmacsha512
```

- (Optional) To enable deprecated algorithms for RAMP CLI, refer to [Enabling Deprecated Algorithms for RAMP CLI](#).

Start

1. Enter the following command on a Linux server:

```
ssh -p 8122 <RAMP username>@<RAMP ID address>
```

Example:

```
ssh -p 8122 cliuser@10.11.22.33
```

Example output:

```
The authenticity of host '[<RAMP ID address>]:8122 ([<RAMP ID address>]:8122)'
can't be established.
RSA key fingerprint is <fingerprint>.
Are you sure you want to continue connecting (yes/no)?
```

2. Enter "yes".

Example output:

```
Warning: Permanently added '[<RAMP ID address>]:8122' (RSA) to the list of known
hosts.
Password authentication
Password:
```

3. Enter the password.

Example output:

```
Sonus Insight

Sonus Insight Command Line Interface
Date: <date and time>
```

4. Enter the following command:

```
f t i
```

Example output:

```
Target           : PSX
Target Version    : V16.01.03
Target Instance   : PSX
Target Instance Version: V16.01.03R000
```

5. Enter the following command:

```
s t i <name of the instance>
```

Example:

```
s t i PSX
```

Example output:

```
Result: Ok
PSX:V14.00.00R000:PSX>
```

6. Configure the PSX device using RAMP CLI. For PSX CLI command examples, refer to [PSX CLI Reference](#).

SBC CLI Through RAMP

The Ribbon Application Management Platform (RAMP) CLI supports executing SBC Core/SLB commands. Perform SSH through port 8122 to enter SBC Core/SLB commands from the RAMP CLI.

Note

The idle timeout interval for a CLI session is set to 30 minutes.

Prerequisites

- **Super User privileges** for **CLI** under **Core Resources**.
- **Super User privileges** for **Configuration Management** under **Core Resources**.
- **Administrator privileges** for the **SBC API/CLI Access Role** under the **SBC Provisioning Role for API and CLI**.
- The SBC Core/SLB device is registered on RAMP.
- The SSH client supports at least one of the following Ciphers/Kex/MACs:
- Ciphers:

```
aes-192ctr
```

- Kex:

```
ecdh_sha2_nistp384  
ecdh_sha2_nistp521  
diffie_hellman_group14_sha1  
diffie_hellman_group14_sha256
```

- MACS:

```
hmacsha256  
hmacsha512
```

- (Optional) To enable deprecated algorithms for RAMP CLI, refer to [Enabling Deprecated Algorithms for RAMP CLI](#).

Start

1. On a Linux server:

```
ssh -p 8122 <RAMP username>@<RAMP ID address>
```

Example:

```
ssh -p 8122 cliuser@10.11.22.33
```

Example output:

```
The authenticity of host '[<RAMP ID address>]:8122 ([<RAMP ID address>]:8122)'
can't be established.
RSA key fingerprint is <fingerprint>.
Are you sure you want to continue connecting (yes/no)?
```

2. Enter "yes". The following message displays:

```
Warning: Permanently added '[<RAMP ID address>]:8122' (RSA) to the list of known
hosts.
Password authentication
Password:
```

3. Enter the password. The following message displays:

```
Sonus Insight

Sonus Insight Command Line Interface
Date: <date and time>
```

4. Run the following command:

```
f t i
```

Example output:

```
Target           : SBX5K
Target Version    : V01.00.00
Target Instance   : sbc
Target Instance Version: V10.01.00R000
```

5. Run the following command:

```
s t i <name of the instance>
```

Note

At times, the `s t i` command fails to connect to the SBC CNF post switchover. Hence it is recommended to re-run the `s t i` command to successfully connect to the SBC shell admin prompt. This happens due to the change of the SSH host key on the SBC CNF after a switchover.

Example:

```
s t i SBX5K
```

Example output:

```
Result: Ok  
SBX5K:V10.01.00R000:SBC>
```

6. Enter the commands for the SBC/SLB device. For information on SBC Core CLI commands, refer to the [SBC CLI Reference Guide](#).

Provision SBC Devices

In this section:

- [Provision SBC Core](#)
- [Compare Uploaded Configurations for SBC Core or SLB Devices](#)
- [Provision SBC Edge Devices](#)

You can provision SBC devices using a predefined configuration through **Ribbon Application Management Platform (RAMP)**. This enables a system administrator to provision multiple devices at a time to apply configuration changes.

RAMP supports provisioning SBC Core, SLB, and SBC Edge devices.

Provision SBC Core

You can partially provision (change the configuration of one or more objects) an SBC Core device that was manually registered, by adding a SIP Message Manipulation (SMM) profile through **Ribbon Application Management Platform (RAMP)**. For more information on SMM, refer to [SIP Message Manipulation](#).

Use partial configurations to make incremental changes.

RAMP contains the latest configuration templates [that were saved on RAMP for every SBC release](#). Choose the software version compatible with the device you want to provision.

Note

During SBC HA switchover, partial configuration provisioning is not supported. Any partial configuration download process in progress may fail due to non-availability of web services.

The dates and times you configure in templates are relative to the RAMP server time zone and not relative to your local time.

SIP Message Manipulation (SMM) configuration profiles are idempotent. That is, if you associate the profile multiple times, it will not have any additional impact.

Prerequisites

- The SBC Core are registered on RAMP.
- You must have **GUI** and **Configuration Management** [privileges](#) under **Core Resources**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Operations > Provisioning > Partial Configurations > Setup**. The **Setup** window displays.
3. Click **New Configuration**. The **New Configuration** pane appears.
4. Select the action you want to perform under the **How do you want to create a configuration?** option.
 - To select a configuration template from the RAMP database:
 - i. Click the **Select Option**.
 - ii. Enter a name for the configuration in the **New Configuration Name** field.
 - iii. Select a profile from **Configuration Type** list. Currently, only the SIP Adaptor (SMM) Profile is available.
 - iv. Select the type of the device to which you want to associate the configuration from the **Node Type** list.
 - v. Select the software version of the SBC Core device to which you want to associate the configuration from the **Node Software Version** list. If there is no exact match for your SBC Core version, a Configuration Template from the closest (lower) version will be used. For example, if 11.00.01R000 is unavailable, 10.00.00R000 template will be used.
 - vi. Select a template from the **Select Configuration Template** list.
 - vii. Click **Save**.
 - To create a configuration by uploading a local file:
 - i. Click the **Upload** option.
 - ii. Enter a name for the configuration in the **New Configuration Name** field.
 - iii. Choose the Node Software Version from the drop-down list.
 - iv. In **Select file to upload** click **Browse for file** to select the file and click **Open**.
 - v. Click **Upload**.
 - To create a new configuration:
 - i. Click **Create** option.
 - ii. Enter a name for the configuration in the **Configuration Name** field.
 - iii. Select a profile from **Configuration Type** list. Currently, only the SIP Adaptor (SMM) Profile is available.
 - iv. Select the device type to associate the configuration, from the **Node Type** list.
 - v. Select the software version of the SBC device to associate the configuration, from the **Node Software Version** list.
 - vi. Click **Create Configuration**. The **SMM** window in **SBC Configuration Manager** appears.
 - vii. Click **SIP Adaptor (SMM) Profile** to open the **SIP Adaptor (SMM) Profile** window.
 - viii. Click **New SIP Adaptor Profile**. The **Create New SIP Adaptor Profile** pane is displayed.
 - ix. Enter a name for the SIP Adaptor Profile in the **Name** field.
 - x. Set criteria.
 - xi. Click **Save**.
 - xii. Click **Save and Close**.

Note

When you create a partial configuration with a SIP Adaptor Profile, the configuration is saved on RAMP if there is at least one SIP Adaptor Profile created. You cannot save an empty configuration file that is a candidate for provisioning. You cannot delete the only entry in the configuration through the SBC Configuration Manager. Instead, you can delete the complete configuration.

5. You can edit a configuration in the **Configuration list** tab. Click the **edit** button under Actions against each configuration. A new window <Configuration name> appears.
 - a. You can view the **Name** of the configuration, **Node Type**, **Node Software Version**, **Configuration Type**, **Created Date/By**, **Last Edited Date/By**.
 - b. Click **Edit Configuration** button to edit the configuration. Click **Cancel** to go back and click **Save** to save the configuration in the configuration list.
6. Create a Target Set, a set of zones and trunk groups, with which to associate the configuration:
 - a. Navigate to **Operations > Provisioning > Partial Configurations > Targets**. The **Target** window displays.
 - b. Click **New Target Set**. The **New Target Set** area is displayed.
 - c. Enter a name for the Target Set in the **Name** field.
 - d. In the **Available Zone**, the list of Zones available are displayed in the **Available** table. Click the **Selector** button, to choose the Zone and it gets displayed in the **Selected** table.
 - e. In the **Available Trunk Group**, the list of available Trunk Groups are displayed in the **Available** table. Click the **Selector** button, to choose the Trunk Group and it gets displayed in the **Selected** table.
 - f. Click **Save**.
 - g. You can **Delete**, **Duplicate** and **edit a Target Set Name** using the Action Buttons.

Note

You can provision one SMM profile for a maximum of 512 trunk groups per single SBC node. To provision a SMM profile for more than 512 trunk groups per SBC node, create another Target Set.

7. Provision the devices:
 - a. Navigate to **Operations > Provisioning > Partial Configurations > Setup**. The **Setup** window displays.
 - b. Click the **Configuration List** tab.
 - i. You can view the **Configuration name**, **Version**, and select the **Configuration type**.
 - ii. You can Provision a configuration, duplicate a configuration, edit a configuration and delete a configuration using the Action buttons.
 - iii. Click **New Configuration** to create a new configuration.
 - c. After a new configuration is created, select the **Provision Configuration** action button against the configuration. You can provision the device using two ways: **Provision** and **Stage**.
 - i. In the Job Type, choose **Provision**.
 1. Enter the **Job Name**, select the **Target Set**, and the **SMM Profile Direction**.
 2. You can schedule to provision the configuration immediately or later using the **Schedule** Option. Enter the **Date** and **Time** to schedule it.
 3. Click **Next**.
 4. **Provision Configuration for** <configuration name> pane is displayed.
All the profiles available in the Target set are listed here.
 - a. If the selected profile exists on a node in the Target Set, the existing profile will be replaced by the new profile.

- b. If the selected profile does not exist on any node in the Target Set, the profile is moved on the selected nodes.
5. When you add a new job, a warning message is displayed stating that the profile doesn't exist on any of the selected node and the provisioning jobs will move the profile on the selected nodes.
6. Once a new job is added, a table with information about the existing profile and the new profile that gets added, along with the Target name and SBC name, is displayed.
7. Click **Save**.
- ii. In the Job Type, choose **Stage**.
 1. Enter the **Job Name**, select the **Nodes**, or the **Resource Groups**.
 2. You can schedule to provision the configuration immediately or later using the Schedule option. Enter the **Date** and **Time** to schedule it.
 3. Click **Next**.
 4. When you add a new job, a warning message is displayed stating that the profile doesn't exist on any of the selected node and the provisioning jobs will move the profile on the selected nodes.
 5. Click **Save**.
8. Click the **Provisioning Jobs** tab.
 - a. You can view the **Job name**, **Configuration**, **Target Set**, **Time**, and **Status**.
 - b. You can Delete a job, view the status of the job using the Action buttons.

Note

You can edit a job that are scheduled for the future.

- i. You can view the **Node Type**, **Node Software Version**, **Configuration Type**, **Created Date/By**, **Last Edited Date/By**. Click **Edit Job** to edit the job type, target set, nodes. frequency etc.
 - ii. Click **View Status** under Actions to view the Provisioning job Status such as **Node Name**, **Time**, **Status**, **Status Details** for each configuration.
9. To check the provisioning status, navigate to **Operations > Provisioning > Provisioning Status**.
 - a. You can view the **Configuration** name, **Node Type**, **Job Name**, **Time** and **Status**.
 - b. Click the expand button on each configuration to view the **Node Name**, **Time**, **Status**, and **Status Details**.

Compare Uploaded Configurations for SBC Core or SLB Devices

You can upload SBC Core/SLB configurations to Ribbon Application Management Platform (RAMP) to edit, duplicate, and compare the uploaded configurations. Either upload a local copy of a configuration file (in XML format) or upload configurations directly from an SBC Core/SLB device registered on RAMP.

Up to 100 SBC Core/SLB configurations can be stored in RAMP.

If the SBC Core/SLB node from which the configuration uploaded is not reachable, comparison does not work. If the SBC Core/SLB node from which the configuration uploaded is upgraded to a new version and the SBC Core/SLB version is not updated on RAMP, discover the SBC /SLB device.

Prerequisites

- The SBC Core or SLB devices are registered on RAMP.
- You must have **GUI** and **Configuration Management** [privileges](#) under **Core Resources**.

Start

1. Log on to the RAMP GUI.

2. Navigate to **Operations > Provisioning > Full Configurations > SBC Core or SLB**. The "Configuration List" window displays.
 - a. The configuration list displays details such as Configuration name, Node name, Node subtype, Version, Date uploaded, and Date last modified.
 - b. You can download, delete, or duplicate a configuration using the **Action** buttons.
 - c. Click **Upload Configuration**. The "Upload Configuration" area displays.
 - d. Enter a configuration name in the **Name** field.

Note

When uploading from an offline copy, the default value is the name of the configuration file.

The default value is <node_name>_<yyyy_mm_dd_hh_mm_ss> (where the date / time when the configuration is uploaded) when the file is uploaded from a node.

3. Perform one of the following:
 - To upload a local copy of a configuration file (in XML format) into RAMP:
 - i. Select the **Upload from Disk** option.
 - ii. Enter the **Name**, Choose the **Version** and browse the file to upload it.
 - iii. Click **Save**.
 - To upload the configuration directly from a manually registered SBC Core/SLB device:
 - i. Select the **Upload from SBC**.
 - ii. Enter the **Name** and select the SBC from **Choose from the list** field.
 - iii. Click **Save**.
4. To edit an uploaded configuration:
 - a. Select an uploaded configuration.
 - b. Click **Edit Configuration**. **Ribbon SBC Configuration Manager / Edit Configuration**. **Ribbon SLB Configuration Manager** window displays.
 - c. Modify the configuration.
 - d. Click **Apply Saved Changes and Close**.
 - e. Click **Save and Close**.
 - f. Click **Save** in the **Edit** <configuration name> area.
5. Select the **Compare** checkboxes for two configurations you want to compare. The first configuration you select is set as the source.
6. Click **Compare Configurations**. The "Configuration Comparison" area appears. Perform one of the following:
 - Click **Full Configurations** under **How to Compare?** to compare complete configurations.
 - Click **Individual Perspectives** under **How to Compare?** to compare configurations by perspective:
 - i. Select a perspective from the list. Refer to the [EMA User Guide](#) for more information.
7. Click **Display Differences**. The "Configuration Comparison" area displays.
8. Hover over an entry in the "Configuration Differences" table to view the path of the object.

Parameters in Configuration Differences

Column	Description
Operation	The operation can be any of the following: ◦ Append ◦ Insert ◦ Delete ◦ Update

Column	Description
Object Type	The type of configuration object that is appended, inserted, deleted, or updated.
Instance Name/Index	The identifier of the object that is appended, inserted, deleted, or updated.
Attributes	Click Show Info to view the attributes of the object that is appended, inserted, deleted, or updated.

9. To download the comparison report in PDF, CSV, or XML format, select the report format from the Download Diff Report list.

Provision SBC Edge Devices

You can provision SBC Edge devices through Ribbon Application Management Platform (RAMP). This allows the system administrator to configure multiple SBC Edge devices simultaneously.

For more information on SBC Edge configuration, refer to [Configuring the SBC Edge System](#).

Note

After an upgrade, the SBC Edge nodes take 5 minutes to be in Online state.

Prerequisites

- The SBC Edge devices are registered on RAMP.
- **GUI** and **Configuration Management** [privileges](#) under **Core Resources**.

Start

1. Log on to the [RAMP GUI](#).
2. Perform one of the following to either upload a configuration file or create a configuration from the backup file:
 - Upload a configuration file

Note

Unzip the downloaded configuration file. The `.xml` file in that folder is to be uploaded.

- i. Navigate to **Operations > Provisioning > Full Configurations > SBC Edge**. The **SBC Edge** window displays.
- ii. Click the **Full Configurations** tab.
 1. Click **Upload Configuration**. The **Upload SBC Edge Configuration** area displays.
 - a. Enter a configuration name in the **Name** field.
 - b. Select the device type from the **Node Sub-Type** list.
 - c. Drag and drop the file in the space provided or Click **Browse for file** to select a `.xml` file from the system.
 - d. Click **Upload**.

- e. The confirmation message, **Configuration uploaded successfully** displays.
- iii. In the **Configurations** list, select a configuration to provision.
 1. Enter the **Job Name** in the job field.
 2. The list of available nodes is displayed in the picklist. You can add or remove the required nodes by using the selectors.
 3. The list of selected nodes is displayed in the **Selected** table.
 4. The list of available Resource groups is displayed in the picklist. You can add or remove the required resource groups by using the selectors.
 5. The list of selected Resource groups is displayed in the **Selected** table.

Note

The Groups list appears only if you have a Resource Group associated with your user group. The “All/Root” resource group does not count. To see a Resource Group in the drop-down list, create a Resource Group, go to the User Group screen, and associate that Resource Group with your User Group.

Note

The provisioning schedule settings of a resource group are applicable to all the nodes assigned under the resource group.

6. In the **Provision Configuration**, do one of the following:
 - To provision the configuration instantly, click the **Now** in **Schedule**.
 - To provision the configuration later, click **Later** in **Schedule** and set a date and time.
7. Click **Save**.
- iv. Go to **Provisioning Jobs** tab.
 1. You can view the **Configuration, Node Sub-type, Job Name, Date/Time** and **Status**.
 2. You can delete a job, edit a job using the Action buttons.

Note

Only the scheduled jobs can be edited. The completed jobs cannot be edited.

- v. You can Download a configuration, delete a configuration, and edit the name of the configuration using the Action buttons.
- Create a configuration from an **SBC Edge backup** file available in RAMP:
 - i. Navigate to **Operations > Backup > Backup Catalog**.
 - ii. Select a backup file.
 - iii. Click **Create Configuration from Backup**.
 - iv. You can view the configuration in the SBC Edge and this can be provisioned.

Back Up and Restore SBC and SLB Devices

In this section:

- [Take Backup of SBC Edge Devices](#)
- [Take Backup of SBC Core and SLB Devices](#)
- [SBC Edge Devices Catalog Management](#)
- [SBC Core and SLB Catalog Management](#)
- [Backup Catalog](#)

Ribbon Application Management Platform (RAMP) supports backup and restore of SBC Core, SLB, and SBC Edge devices simultaneously.

RAMP acts as a repository for your device backup. The system backup files contain configuration data and other binary or ASCII files. You can retrieve the system files from the servers of the managed device. The generated files are stored on the RAMP database.

If a scheduled backup fails for one or more devices within a backup schedule, an alarm will be raised indicating the failure.

Take Backup of SBC Edge Devices

The Ribbon Application Management Platform (RAMP) supports taking backup files from SBC Edge devices to enable restoring the device if necessary. You can select which resources to back up and how frequently RAMP takes the backup.

Prerequisites

- The SBC Edge device is registered on RAMP.
- **Devices** [privileges](#) under **Device Management**.
- **Super User** [privileges](#) under **GUI** and Configuration Management in **Core Resources**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Operations > Backup > Scheduled Backups**. The **Scheduled Backups** window opens.
3. Click the **Backup Status** tab to view the backup status list. This is a read-only list. You can view the **Job Name, Node, Node Type, Subtype, Backup Start Date/Time, and Status**.
4. Click the **Scheduled Backups** tab to view the Scheduled Backup list. You can view the **Name, Frequency, Backup Start Date/Time, and Status**.
 - a. From the Actions buttons, you can Delete a scheduled backup, run backups, and Edit a Backup.
5. Click **Create Backup Schedule** to open **Create Backup Schedule** options.
6. Enter a name in **Job Name**.
7. Select a backup frequency from the Run Backup options such as **Daily, Weekly** and **Now**.
 - a. If the **Daily** option is selected, enter the backup start time in **Starts at**. **Start time is set as per RAMP time zone set in the RAMP time server**. RAMP backs up the device configuration every day at the set time.
 - b. If the **Weekly** option is selected, select a backup date from the **Date** field and enter the backup start time in **Starts at**. RAMP backs up the device configuration every week based on the set date and time.
 - c. If the **Now** option is selected, **RAMP takes a backup of the system configuration immediately**.
8. Select one or both of the following:
 - From the **Nodes** list, select the nodes on which you want to perform backup.
 - From the **Groups** list, select the resource groups on which you want to perform backup. A Resource Group list is displayed only if you have a Resource Group associated with your user group. The **All/Root** resource group does not count. If you want to see a Resource Group, create a Resource Group, and then go to the User Group screen and associate that Resource Group with your User Group. Then, you will see the Resource Group in the list. When you select a resource group, the backup schedule is applicable to all the nodes in the resource group.

9. Click **Save**.

If the backup succeeds for all nodes, a success message displays. If the backup fails for one or more nodes, a fail message displays.

Take Backup of SBC Core and SLB Devices

Ribbon Application Management Platform (RAMP) supports taking backup files from manually registered SBC Core and SLB devices to enable restoring the device if necessary. You can select which resources to back up and how frequently RAMP takes the backup.

Prerequisites

- The SBC Core/SLB devices are registered on RAMP.
- **Devices** [privileges](#) under **Device Management**.
- **Super User** [privileges](#) under **GUI and Configuration Management** in **Core Resources**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Operations > Backup > Scheduled Backups**. The **Scheduled Backup** window displays.
3. Click the **Backup Status** tab to view the backup status list. This is a read-only list. You can view the **Job Name**, **Node**, **Node Type**, **Subtype**, **Backup Start Date/Time**, and **Status**.
4. Click the **Scheduled Backups** tab to view the Scheduled Backup list. You can view the **Name**, **Frequency**, **Backup Start Date/Time**, and **Status**.
 - a. From the **Actions** buttons, you can delete a scheduled backup, run backups, and edit a backup.
5. Click **Create Backup Schedule** to open **Create Backup Schedule** options.
6. Enter a name in **Job Name**.
7. Select a backup frequency from the **Run Backup** options such as **Daily**, **Weekly** and **Now**.
 - a. If the **Daily** option is selected, enter the backup start time in **Starts at**. RAMP backs up the device configuration every day at the set time.
 - b. If the **Weekly** option is selected, select a backup date from the **Date** field and enter the backup start time in **Starts at**.
The RAMP backs up the device configuration every week based on the set date and time.

Note

For Daily/Weekly backups, you can run them manually without waiting for it to run at the specified time during creation.

- c. If the **Now** option is selected, RAMP takes a backup of the system configuration immediately.
8. Select one or both of the following:
 - From the **Nodes** list, select the nodes for which you want to perform backup.
 - From the **Groups** list, select the resource groups for which you want to perform backup.

Note

A Resource Group list is displayed only if you have a Resource Group associated with your user group. The All/Root resource group does not count. If you want to see a Resource Group, create a Resource Group, and then go to the User Group screen and associate that Resource Group with your User Group. Then, you will see the Resource Group in the list.

Note

When you select a resource group, the backup schedule is applicable to all the nodes in the resource group.

9. Click **Save**.

Note

If the backup succeeds for all nodes, a success message displays. If the backup fails for one or more nodes, a fail message displays.

SBC Edge Devices Catalog Management

Ribbon Application Management Platform (RAMP) supports restoring SBC Edge devices using backup files stored in the RAMP database. You can view the backup catalog, create a configuration from the backup and download the catalog. You cannot search for backup files on the RAMP disk.

After an upgrade, the SBC Edge nodes take approximately five minutes to come online.

Prerequisite

- The devices are registered on RAMP.
- **Devices** [privileges](#) under **Device Management**.
- **Super User** [privileges](#) for **GUI** and Configuration Management in **Core Resources**.
- Ensure that the device backup is available on RAMP. To take a backup of an SBC Edge device, refer to [Take Backup of SBC Edge Devices](#).

Start

1. Log on to the RAMP GUI.
2. Navigate to **Operations > Backup > Backup Catalog**. The **Backup Catalog** window opens.
3. The list of all Backup catalogs is displayed.
 - a. Use the **Action** buttons to download or restore a backup. For more information on Backup Catalog, refer [Backup Catalog](#).
4. To create a configuration from the existing backup:

- a. In the backup catalog, select the node to create the configuration.
- b. Click **Create Configuration from Backup**. A confirmation dialog box appears.
- c. Click **Yes** to create a new configuration. A message appears after the new configuration is successfully created.

The new configuration is created in Full Configuration -> SBC Edge.

5. Select the download button for the catalog you want to download. A prompt message asking If you want to download this backup to disk will appear.
6. Click **Download** to download the catalog or click **Cancel** to cancel the action.
7. Select the Restore button for the catalog you want to restore.
8. When prompted, confirm you want to restore backup for <Node name>.
 - a. Click **Restore** to restore the backup or click **Cancel** to cancel the action.

SBC Core and SLB Catalog Management

Ribbon Application Management Platform (RAMP) supports restoring SBC Core/SLB devices using backup files that are stored in the RAMP database. You can view the backup catalog and download the catalog. However, you cannot search for backup files on the RAMP disk as the backups are maintained in the database.

Prerequisites

- The devices are registered on RAMP.
- Ensure that the device backup is available on RAMP. To take backup of SBC Core/SLB devices, refer to [Take Backup of SBC Core and SLB Devices](#).
- Super User [privileges](#) for GUI and Configuration Management under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Operations > Backup > Backup Catalog**. The "Backup Catalog" window displays.
3. **Download:**
 - a. Use the **Action** button to download or restore the backup. For more information on Backup Catalog, refer [Backup Catalog](#).
 - b. Select the download button for the Catalog you want to download.
 - c. When prompted, confirm you want to download this backup to the disk.
 - d. Click **Download** to download the Catalog or click **Cancel** to cancel the action.
4. **Restore:**
 - a. Select the **Restore** button for the catalog you want to restore.
 - b. When prompted, confirm you want to restore the backup for <Node name>.
 - c. Click **Restore** to restore the backup or click **Cancel** to cancel the action.

Backup Catalog

A catalog of device backups is maintained for each managed Network Element.

The following information will be maintained for each device backup within the catalog:

- The Network Element whose configuration was backed up.
- Date and Time of the backup.
- The software release the device was running at the time the backup was taken.

You can retrieve a backup from the catalog, via https download, for offline use.

Backup retention is as follows:

- One backup from the previous major release the node was running.
- One backup per day for one week.
- One backup per week for one month.

Remaining backups are deleted to maintain the storage space.

Retrieving a backup from the catalog requires Super User or Administrator permission to the network elements whose backups are being retrieved.

You can create a device configuration from a backup (applicable for SBC Edge devices only), download a backup, and restore the device configuration using Backup Catalog.

Upgrade SBC Devices

Contents

- [Upgrade SBC Core](#)
- [Upgrade SBC Edge](#)
- [Upgrade SLB](#)

You can upgrade SBC Core, SBC Edge, and SLB devices using the Ribbon Application Management Platform (RAMP) GUI. SBC upgrade through RAMP requires manually uploading the upgrade files to RAMP. RAMP retains the older versions of the device and supports rollback.

In a RAMP redundancy set-up, the upgrade files are automatically copied from the active device to the standby device. The upgrade images are available on both devices. Upgrade will not be interrupted even if a switchover occurs on RAMP, after the switchover you can check the upgrade status in the active RAMP device (new).

Do not unregister a node from RAMP during the upgrade. Before unregistering a node, remove it from the upgrade schedule.

Upgrade SBC Core

You can upgrade SBC Core standalone and HA devices using images you upload to Ribbon Application Management Platform (RAMP).

Ribbon recommends that you execute network-wide upgrades serially. You can schedule multiple automated upgrades to stagger the upgrades of your SBC 5x00, SBC 7x00, and SBC SWe so that if one upgrade fails, the next element does not upgrade.

The BMC firmware is not dependent on the SBC application.

Upgrades of SBC 5x00 and SBC 7x00 devices with the Baseboard Management Controller (BMC) service processor running must be performed independently using Platform Manager.

Both nodes in an HA pair must be up and have the application running for the upgrade to proceed. After an SBC upgrade is complete, the roles of the nodes in an SBC HA pair are reversed:

- The active node becomes the standby node.
- The standby node becomes the active node.

Image Type	Device Version
gzipped tar (OS, application, and BIOS)	V06
signature	V06
MD5 The md5 file is applicable only for upgrading the SBC nodes from pre-9.0 versions to 9.0 and later.	V06
sha256 The sha256 file is applicable only for upgrading the SBC nodes from 9.0 and later releases.	V09
qcow2	V06

Upgrade SBC Edge

You can upgrade SBC Edge devices using images you upload to Ribbon Application Management Platform (RAMP).

To communicate with ASM for an SBC 1000/SBC 2000 node, [Upgrade the SBC Communication Service Version](#) before upgrading the Ribbon SBC Edge software.

The ASM may become unavailable if you upgrade Ribbon SBC Edge firmware before upgrading SBC Communication Service Version on SBC 1000/SBC 2000.

Image Type	Device Version
SBC 1000/SBC 2000 application	3.0 or later
SBC 1000/SBC 2000 boot	7.0.1 and later
SBC 1000/SBC 2000 ASM	3.1 or later
Microsoft Direct Routing SBA	version 2022-06-14 onwards.

Upgrade SLB

You can upgrade manually registered SLB devices using images you upload to Ribbon Application Management Platform (RAMP).

Ribbon recommends that you execute network-wide upgrades serially. You can schedule multiple automated upgrades to stagger the upgrades of SLB devices so that if one upgrade fails, the next element does not upgrade.

Prerequisites

- You must have Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- You must have **Devices** and **Resource Groups** [privileges](#) under **Device Management**.
- The SLB devices are registered on RAMP.
- If the SLB version that you want to upgrade to does not have native support on RAMP, obtain the Live Software Upgrade (LSWU) file that contains the SLB version. If the SLB version is released after the RAMP release, RAMP does not support that SLB version.
- The following files are available:

files in upgrade image
gzipped tar (OS, application, and BIOS)
signature
sha256
qcow2

Start

- Log on to the RAMP GUI.

Step 2 is applicable only if the SLB version that you want to upgrade to does not have native support on RAMP.

- Upload the appropriate LSWU file for SLB:
 - Navigate to **System > Settings > Upload LSWU File**.
 - Click **Choose File**.

- c. Browse the file.
 - d. Click **Upload**.
3. Upload the upgrade files:
 - a. Navigate to **Operations > Upgrade > Images**. The **Images** window opens.
 - b. Click **Upload Image**. The **Upload Image** pane opens.
 - c. Click **Choose Files**.
 - d. Select the upgrade image files and click **Open**. Select the `tar.gz`, `signature`, `qcow2`, and `sha256` files all at once.
 - e. Click **Save**.
The uploaded images displays in the **Upgrade Images** area.
4. Schedule the upgrade:
 - a. Navigate to **Operations > Upgrade > Schedules**. The **Schedules** window opens.
 - b. Select an upgrade image file from the **Image Name** list.
 - c. Click **Schedule Upgrade**. The **Node Eligibility** window opens. Eligibility for upgrade is determined based on the device version compatibility Live Software Upgrade (LSWU) matrix.
 - d. Select a device or group of devices (resource group) for upgrade:
 - Click the **Individual Nodes** tab and select a device to upgrade.
 - Click the **Resource Groups** tab and select a resource group to upgrade all the devices nodes in the resource group. When a resource group is selected, only the nodes within that resource group of the required type and eligible versions are upgraded. To view the eligible nodes, click on a resource group.
 - e. Perform one of the following:
 - Drag and drop nodes/resource groups to the **Upgrade Target List**.
 - Select nodes/resource groups and click **Add Target(s)**. The selected targets are listed in the **Upgrade Target List**. To remove a target from the **Upgrade Target List**, click **Remove Target(s)**.
 - f. In **Upgrade Scheduling**, enter a name in the **Job Name** field.
 - g. Select the number of devices to upgrade simultaneously from the **Number Of Simultaneous Upgrades** list. A scheduled job can contain more than 5 nodes. However, RAMP upgrades up to 5 nodes at a time.
 - h. Set whether to terminate upgrade if the upgrade fails on a device:
 - To terminate the upgrade if the upgrade fails on a node, select **Stop On Failure On One Node**. The upgrade jobs that are started on a node are completed. Only the upgrade jobs that are yet to start on a node are cancelled.
 - To continue the upgrade on other nodes even if the upgrade fails on a node, do not select **Stop On Failure On One Node**. If the upgrade fails on a node, an alarm is raised.
 - i. Set whether to reboot the devices immediately after the upgrade:
 - i. **Immediate** - the upgrade is initiated and nodes are rebooted immediately after the upload is completed.
 - ii. **Scheduled** - select a date from the **Date** field and enter time in the **Starts At** field for the upgrade to start and nodes to reboot after the upload. The upgrade starts only when upload is complete, irrespective of the upgrade schedule. The upgrade starts only for the nodes for which the image upload is successful.
5. Click **Save**.
6. Check the upgrade status :
 - a. Navigate to **Operations > Upgrade > Nodes**. The **Nodes** window opens.
 - b. Select the node. The **Version History** <name> pane opens.
 - c. If the upgrade failed, you can restore the device software to an older version, select an older version and click **Rollback Version**. You are prompted to confirm.
 - d. Click **Yes** to confirm.

Generate Health Reports

The Ribbon Application Management Platform (RAMP) provides health reports with information that can help you reduce downtime. You can analyze health reports, along with performance reports, to more closely monitor your network. Monitoring the overall health of the network and devices allows you to prevent connectivity issues and service disruptions.

Use health reports to track resource usage such as hardware alarms, CPU usage, and swap space. This allows you to optimize system and network resources. The metrics can also help you to identify devices and services which are frequently active. Use health reports to determine the overall health of the network with respect to changing traffic demands and operating conditions.

Device and Network Health reports extract data from the performance management (PM) statistics stored in the RAMP database. Refer to [Collect and Export Device Statistics](#). The PM data from devices is used for populating resource usage columns in health reports. The health reports also use alarms with a critical severity reported on RAMP to generate health data.

RAMP has predefined templates for health reports from which you create specific reports for your deployment. You can generate health reports on demand or you can schedule health reports.

Note that device-specific reports (PSX) are generated with no date if the associated devices are not registered on Ribbon Application Management Platform (RAMP).

Use the following procedure to either generate a report immediately (on demand) or schedule it to run in the future.

Prerequisites

- You must have Super User [privileges](#) for **Health Reports** under **Core Resources** to generate and schedule reports.
- You must have Operator or Super User [privileges](#) for **Performance Reports** under **Performance Management** to generate reports.

Start

- Log on to the RAMP GUI.
- Perform one of the following:
 - To generate health reports on demand:
 - Navigate to **Operations > Health Reports > On Demand**.
 - Expand the tree to see the available templates under **Device and Network Health** and **Inventory**.
 - Select a template for the type of report you want to generate. Refer to the following table for the templates.
 - Enter a name for the report in **Report Name** and optionally enter a **Description**.
 - Select a **Time Range**.
 - Refer to the following table for the additional parameters to enter for each type of report template.

Report Parameters

Report Template Name	Parameters
Device and Network Health	

Report Template Name	Parameters
GSX Health Report	The GSX Health report filters GSX information based upon the time duration you specify, your selection of either unacknowledged Critical Alarms (0) or All Critical Alarms (1), and thresholds you set for the parameters listed below. ◦ MC1 Transitions Count for Processors ◦ MC2 Transitions Count for Processors ◦ MC3 Transitions Count for Processors ◦ Calls Receiving No-Circuit Treatment ◦ Outgoing Trunk Start Signal Timeouts ◦ Misc. Ineffective Machine Attempts ◦ Vacant Code Treatments ◦ Call Attempt Failures ◦ Call Attempts Blocked
GSX Softswitch Health Report	The GSX Softswitch Health report filters information concerning communication between GSX(s) and PSX(s) based upon the time duration you specify and thresholds you set for the parameters listed below. ◦ Server Reconnects ◦ Transaction Retry Attempts ◦ Transaction Failed Attempts
Insight Health Report	The Insight Health report filters RAMP information based upon the time duration you specify, your selection of either unacknowledged Critical Alarms (0) or All Critical Alarms (1), and thresholds you set for the parameters listed below. ◦ Average CPU Usage (%) ◦ Average Swap Space Usage (%)
Overall Network Health Report	The Overall Network Health report lists all nodes that are currently experiencing potential issues. The report displays the node name, node type, and the number of outstanding events. Unlike other health reports, you do not need to set any filtering criteria. Simply enter a name and save the report to make it available. RAMP automatically filters all registered nodes based upon outstanding critical alarms.
PSX Applications Health	The PSX Application Health report filters PSX information upon the time duration you specify and the threshold you set for Average CPU Usage (%).

Report Template Name	Parameters
PSX Health	The PSX Health report filters PSX information based upon the time duration you specify, your selection of either unacknowledged Critical Alarms (0) or All Critical Alarms (1), and thresholds you set for the parameters listed below. ◦ Average CPU Usage (%) ◦ Average Memory Usage (%).
Inventory	
Devices Version Summary	This report shows the number of device on a particular software version. The device count is grouped by the type of device.

- vii. Click **Save**. The report is saved under the **Saved** section of the Report tree.
- viii. To run the report, select it from under **Saved** and click **Run**. The report displays in a new window.
- To set up reports to generate at specified intervals on a recurring basis:
 - i. Navigate to **Operations > Health Reports > Scheduled**.
 - ii. Expand the tree to see the available templates under **Device and Network Health** and **Inventory**.
 - iii. Select a template for the type of report you want to schedule. Refer to the previous table for the templates.
 - iv. Enter a name for the report.
 - v. Schedule **how frequently you want to run the report**.
 - vi. Select a time range during which you want to run the report.
 - vii. Refer to the previous table for additional parameters for each report type.
 - viii. Click **Save**. The report is saved and runs when scheduled.
 - ix. After the scheduled time, select your report name under **Currently Scheduled** reports. The report displays in a new window.

Lock and Unlock Devices

In this section:

- [Lock a Device](#)
- [Review Which Devices are Locked](#)
- [Unlock a Device](#)

You can lock GSX or SBC Core devices on Ribbon Application Management Platform (RAMP) to prevent write access, or both read and write access, to the device by other users. A locked device unlocks automatically if the user who locked the device logs out from RAMP or can be unlocked by another user with sufficient privileges to work with node locking.

Prerequisite

You must have Super User [privileges](#) for **Insight Administration** under **Core Resources**.

Lock a Device

Use the following procedure to lock a GSX or SBC Core device.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Operations > Manage Node Locks**.
3. Select the **Set Node Lock** tab.
4. Select a device from the **Selected Node** list. The **Current Lock State** displays the state of the selected node.
5. From the **Desired Lock Setting**, perform one of the following :
 - To prevent modifying the device, select **Lock for write access only**.
 - To prevent access to the device, select **Lock for read and write access**.
6. Click **OK** or **Apply** to lock the device. Locked devices are listed in the **Locks in Effect** tab.

Review Which Devices are Locked

Use the following procedure to check which nodes are currently locked.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Operations > Manage Node Locks**.
3. Select the **Locks in Effect** tab. RAMP lists the locked nodes, if any.

Unlock a Device

Use the following procedure to lock a GSX or SBC Core device.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Operations > Manage Node Locks**.
3. Select the **Set Node Lock** tab.
4. Select the locked device from the **Selected Node** list.
5. Select **Unlock**.
6. When prompted, confirm that you wanted to unlock the device.

Automate Configuration Tasks for GSX

In this section:

- [Launch GSX Task Configurator](#)
 - [View Task Details](#)
 - [Add a Task to the Task List](#)
 - [Edit a Task](#)
 - [Copy a Task](#)
 - [Delete a Task](#)
 - [Disable or Enable a Task](#)
 - [Schedule a Task](#)
 - [Run a Task List](#)
 - [Troubleshoot Tasks](#)
 - [Create a New Template Task List](#)
 - [Create a Node-Specific Task List](#)
 - [Add Comments to a Task List](#)
 - [Validate a Task List](#)
 - [Save a Task List](#)

Related articles:

- [Task Definitions](#)

- [Import a Template into a Task List](#)
- [Task List Management](#)
 - [Launch Task List Management](#)
 - [Convert a Task List](#)
 - [Delete a Task List](#)
 - [Export a Task List from the RAMP Database](#)
 - [Import a tcl file or Exported Task List to the RAMP Database](#)
- [View Configurator Logs](#)

The **GSX Task Configurator**, available from **Ribbon Application Management Platform (RAMP)**, allows you to develop and run task lists (CLI scripts) to automate the configuration of new GSX switches and to perform repetitive configuration tasks on switches already in service.

Note

Task lists are synonymous with CLI scripts, while individual tasks in a list are synonymous with Tcl procs containing CLI commands.

The **GSX Task Configurator** options display in the RAMP GUI only if a GSX device is registered on the RAMP.

The options available under **GSX Task Configurator** are:

- **Task Configurator**
To create, save, and run scripts. The commands available to each user are based upon their privilege level.
- **Task List Management**
To convert task lists created for older versions of the GSX to lists that are compatible with newer versions, and to delete lists.
- **Logs**
To view logs of operations conducted on each task list.

You can create task lists using GSX command line interface (CLI) commands as building blocks. You can modify, delete, or copy tasks within a task list. After you create the task list, you can validate, troubleshoot, run (against a switch), and save (for future use or adaptation) the task list. RAMP provides several task list templates to assist you in getting started and creating new task lists.

Launch GSX Task Configurator

Use the following procedure to launch the GSX Task Configurator.

Prerequisites

- You must have Super User [privileges](#) for **Configuration Management** under **Core Resources** to add and edit tasks.
- Users with Provisioner [privileges](#) for **Configuration Management** under **Core Resources** can only validate and run task lists, enable and disable tasks, view the details of a task, and view logs.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Operations > GSX Task Configurator > Task Configurator**. The **Task Configurator** window displays.
3. Select the appropriate type and version of the GSX that you want to configure. The **Task Lists** list updates, displaying only those task lists available for the version selected.

The **Task Lists** menu on the toolbar contains all of the saved task lists. The system orders each category and the tasks within their running sequence. You cannot change the order. This order also represents the recommended sequence for editing a task list.

You can open multiple task lists, edit them, and move between the lists by selecting the lists from the **Task Lists** drop-down menu. Close a task list by clicking the **X** icon at the top right of the list. When closing a list or exiting the Configurator, the system prompts you to save changes.

You can either scroll through the list to locate a specific task or click one of the links to the right of the task list in the **Jump to Category** bar to move to a selected category in the task list. To hide task categories that do not contain tasks, select the **Hide empty categories** option. Select a specific task within a task list by selecting the corresponding check box to the left of the task name in the list.

After launching the GSX Task Configurator use the following procedures to work with tasks and task list.

View Task Details

To view the details of a task:

1. Select a task list from **Task Lists**.
2. Select a specific task by checking the check box to the left of the task name in the list.
3. Click the "View details of the selected task" icon in the toolbar.

Add a Task to the Task List

To add a task to a task list:

1. Select a task list from **Task Lists**.
2. Scroll to the category in the task list for which you want to add a task.
3. Select a task to add from the list for task category.
4. Click **Add Task** to open the Add Task window.
5. Enter the appropriate parameters. For information regarding the task (Tcl Proc), click **Help** in the Edit Task window.
6. Click **OK**.
A confirmation message verifies that the parameters you entered are valid.
7. Click **Close**.
The new task is added to the list in the appropriate sequence.

Edit a Task

To edit a task:

1. Select a task list from **Task Lists**.
2. Select a task by checking the check box to the left of the task name in the list.
3. Click **Edit** to open the Edit Task window with the current parameters of the task shown.
4. Change the parameters as necessary. For information regarding the task (Tcl Proc), click **Help** in the Edit Task window.
5. Click **OK**.

Copy a Task

To copy a task:

1. Select a task list from **Task Lists**.
2. Select a specific task by selecting the check box to the left of the task name in the list.
3. In the toolbar, click **Copy**.
A copy of the task will appear in the task list below the selected task. It can then be edited.

Delete a Task

To delete a task:

1. Select a task list from **Task Lists**.
2. Select a task by selecting the check box to the left of the task name in the list.
3. In the toolbar, click **Delete**.

Disable or Enable a Task

Disable specific tasks to prevent them from running when you run the task list.

1. Select a task list from **Task Lists**.
2. Select a task by selecting the check box to the left of the task name in the list.
3. Click the **Disable** icon in the toolbar. Disabled tasks have a grayed-out appearance in the task list.
4. Enable a task by selecting it and clicking the **Enable** icon.

Schedule a Task

The Task Scheduler tab on the Task Configurator screen allows you to schedule GSX Accounting Log Rollovers.

To schedule an Accounting Log Rollover,:

1. Click **Create** on the Task Scheduler screen.
2. In the **Create Scheduling Entry** dialog box, select the GSX(s).
3. Set the Frequency and Start Time.
4. Click **OK**. The new entry appears on the Scheduling page.
You can schedule only one GSX Accounting Log Rollover task. However, you can include multiple nodes.

To modify the settings or to delete the entry, select it and click the appropriate button.

Run a Task List

1. Select a task list from **Task Lists**.
2. Click **Run**. The **Run Task List** window opens. The system automatically locks the node for write access.
3. Select the node that you want to run the task list on from the **Node** list. The version of task list you select determines which GSX nodes display in the **Run Task List** window.
4. Select the commands as follows:
 - Select **Stop on error** if you want the task list to stop running if an error occurs. RAMP maintains a log of the task errors. To access the logs, navigate to **Operations > GSX Task Configurator > Logs**.
 - If there is a specific range of tasks (in the Task List) that you want to run, enter the range in the **Task Range** fields.
 - Click **Run** to run the task list. Unless **Stop on error** is checked, the task list will run in its entirety, regardless of errors encountered.

Click **Abort** to stop running a task list.

Once the task list finishes the node returns to an unlocked state.

When a Task List does not run completely due to an error in the list, the system disables the Tasks that are run successfully. The tasks that did not run successfully remain in an enabled state. When you rerun the task list after debugging any unsuccessful tasks, the system runs only the enabled tasks.

Troubleshoot Tasks

1. Select a task list from **Task Lists**.
The task list displays in the work space area reflecting the tasks contained in the list.
2. Click **Run**. The **Run Task List** windows.
3. Select **Stop on error**.

4. Run the task list. **RAMP** will stop running the task when errors occur. Debug errors by viewing the CLI output, which includes a stack trace indicating the line in the Tcl proc where the error occurred. That information, in conjunction with the proc (task) detail window, can help you pinpoint which CLI command encountered the error, and why.
5. Trace back using the CLI output, to determine why the error occurred. For example, wrong card type.
6. Close the **Run Task List** window (the log is automatically saved). Go to the task list details and modify the parameters of the task that generated the error.
The system disables all tasks that run successfully, so that the successful tasks do not run a second time.
7. Rerun the task list. The task resumes starting with the first task that failed in the previous run.
8. Repeat the above steps until the whole task list completes successfully.

Create a New Template Task List

Task lists can be of two types, templates or GSX-specific. You can run a template task list on any node, while a node-specific task list can only be run on the node for which it was intended.

1. Click the **Create New Task List** icon to open the **New Task List** window.
2. Select **Template Task List**.
3. Provide a name for the task list.
4. Click **OK**.
5. Edit the list as necessary.

The system automatically categorizes all task lists converted from older versions as Template task lists.

Create a Node-Specific Task List

When creating a node-specific task list, the system automatically generates an initial task list based upon the node's hardware inventory.

1. Click the **Create New Task List** icon to open the **New Task List** window
2. Select **GSX Specific Task List**.
3. Enter a name for the list.
4. Select an existing template for the list. Choose the Empty template if you do not want to include a template.
5. Select a node to associate with the task list.
6. Click **OK**.

The system generates a new task list with services included in the template selected, along with tasks for configuring the cards currently present on the node (based on the hardware inventory obtained by querying the node).

Add Comments to a Task List

Use the "Task list notes" tool to add comments to a task list. This can be helpful when multiple users are editing and running the same scripts.

1. Select a task list from **Task Lists**.
2. Click the "Task list notes" icon in the top right corner of the task list.

Validate a Task List

Validation provides data integrity verification of configuration scripts. Currently, this validation routine checks only name references within the scripts and types of tasks that should occur only once in the list (for example, event log definitions).

The system allows you to run a task list that contains validation errors and warnings.

1. Select a task list from **Task Lists**.
2. Click the **Validate** button. The **Validate Task List** window opens.
3. Click **Apply**.

Save a Task List

As there is currently no “autosave” feature, Ribbon recommends periodically saving an open task list. Also, the system does not automatically save changes in a particular task list when a different task list is opened. Modified task lists display in **Task Lists** with an asterisk.

When you save a node-specific task list, the system retains the enabled/disabled status of the tasks. This allows you to revisit partially run scripts at a later time for run completion. The system does not retain this information in a Template task list, since you can run this type of task list on any node.

1. Select a task list from **Task Lists**.
2. Click the **Save task list** icon.

Use the **Save task list with a different name** option to save a task list with a different name. You cannot overwrite original task list templates. You must save new/modified task list templates with a different name. You can save task lists as GSX specific task lists when associated with a specific GSX.

GSX-specific task lists have the GSX ID embedded in them. If the node ID changes, or if you copy a task list from one Insight server to another, the task list may become unexecutable. To recover from this problem, you can save the task list and re-associated it with the correct node ID for the GSX using the **Save task list with a different name** icon.

Import a Template into a Task List

Occasionally, you may need to import a task list template into a newly created or existing task list.

1. Select a task list from **Task Lists**.
2. Click the **Import** icon.
3. Select a template from the list.
4. Click **OK**.

The system imports the tasks into the template in the appropriate sequence.

Task List Management

Users with Super User [privileges](#) for **Configuration Management** under **Core Resources** can use the features in the Task List Management interface to convert task lists from an older version to a newer version, import or to delete task lists.

Launch Task List Management

Use the following procedure to launch Task List Management.

1. Log on to the RAMP GUI.
2. Navigate to **Operations > GSX Task Configurator > Task List Management**. The status of operations performed displays in the status area at the bottom of the window.

After launching the Task List Management interface, use the following procedures.

Convert a Task List

To convert a task list to a different version:

1. In the **Conversion** section of the GUI, select a version from the **Convert from** list.
2. Select the version that you want to convert to from the **Convert to** list.
3. Choose the task list(s) that you want to convert from the **Available** list and move them to the **Selected** list using the **>>** button.
4. Click **Convert**.
After conversion, both the new converted task list and the original version are available from the **Task Configurator**.

Delete a Task List

To delete a task list:

1. In the **Maintenance** section, select a version from the **Version** list.
2. Select the task list(s) that you want to delete from the list.
3. Click **Delete**.

Export a Task List from the RAMP Database

To export task lists from the database to tcl files for transfer to other systems:

1. In the **Import/Export Tasks** section, click the **Export** button to open the **Export task lists** window.
2. In **Select Export Version**, select the software version of the task list you want to export.
3. In **Task lists for the selected version**, select the particular task list that you want to export.
4. Click the **Export** button.

The system creates a file with the same name as the task list exported in the <BASE_DIR>/weblogic/sonusEms/data/X_X/TB/templates directory, where X_X is the **Select Export Version**.

Import a tcl file or Exported Task List to the RAMP Database

To import an older tcl file into the database or to import a tcl file exported from a different RAMP server, perform the following:

You must copy tcl files to import into the correct directory structure. the path is <BASE_DIR>/weblogic/sonusEms/data/X_X/TB, where X_X is the subdirectory representing the software version in which you created the tcl file.

1. In the **Import/Export Tasks** section, click **Import** to open the **Import Task Lists** window.
2. In **Select Import Directory**, select the directory/path where the tcl file(s) you want to import resides.
3. In **Task Lists under the selected directory**, select the task list you want to import to the database.
4. Click **Import**.

The imported task list will now be available from the **Task List** list for the appropriate version.

View Configurator Logs

An historical log of operations performed on each task list is available.

1. Log on to the RAMP GUI.
2. Navigate to **Operations > GSX Task Configurator > Logs**.
3. Select a log file from the **Log** drop-down menu.

If you are examining a larger log file, you can search log output using Find In Page feature in the toolbar.

Task Definitions

In this section:

- [Tasks](#)
 - [Node](#)
 - [Profiles](#)
 - [Servers](#)
 - [OC3 Groups](#)
 - [Events](#)
 - [System Timing](#)
 - [Gateway to Gateway](#)

- NIFs
- Optical Interfaces
- OSPF
- OSPFV3
- ATM
- Static Routes
- Circuits
- Ribbon Softswitch
- MGCP
- H323
- SIP
- Media Gateway
- SS7 Gateway
- Common Provisioning
- LP (Local Policy) Provisioning
- ISUP Provisioning
- BT IUP Provisioning
- ISDN Provisioning
- CAS Provisioning
- IP Provisioning
- GR303 Provisioning
- Diameter Provisioning
- Miscellaneous
- Mtrm Provisioning

This section describes tasks (Tcl Procs) available in Task Configurator within the Ribbon Application Management Platform (RAMP) GUI.

You can run many tasks defined in this section multiple times on a switch to achieve the desired configuration, while other tasks are executed only once. For example, you can rerun a task to place a switch object into service that was configured but intentionally left out of service. Whether a task can or cannot be rerun is defined in the Task Description column below. The following annotations appear in the tables for each task:

- **Rerun:** Y/N specifies if you can rerun the script through the Task Configurator.
- **GSX Nav:** Y/N specifies if the procedure is available through the GSX Navigator.
- Before building task lists,
 - refer to [GSX9000 release notes](#), and
 - configure the GSX so its management interface(s) is operational. During node discovery, RAMP automatically creates a management client on the GSX.
- While building task lists, refer to [GSX Operations Guide and Installation Guide](#).
- You can turn on parameter file loading before or after configuring a GSX using the Task Configurator.
- When the CREATE SERVER commands automatically create NIFs, Circuits, and SONET interfaces, The Task Configurator applies a default naming convention. The RAMP does not currently support any alternate naming convention.
- Some of the tasks defined in this topic are also available from the GSX Navigator depending on the type of object selected in the Navigator tree.

Tasks

The tasks performed on every object in Task Configurator are listed here.

Node

The tasks performed on a node are described in the table below:

Task Name	Task Description
Create Management Client	Creates the named management client with an associated IP address and enables its administrative state. You may define a maximum of 8 management clients. Rerun: Y GSX Nav: N
Create User Profile	Creates the named user profile with an associated password and enables its administrative state. Rerun: Y GSX Nav: N
Create User	Creates the named user with an associated password and enables its administrative state. You may define a maximum of 8 users. Rerun: Y GSX Nav: N
Create User using Profile	Creates the named user with all configuration setting taken from the named profile and enables its administrative state. You may define a maximum of 8 users. Rerun: Y GSX Nav: N
Configure Local Time Zone	Defines the local timezone from a selectable list of zones. Rerun: Y GSX Nav: N
Configure Accounting	Defines the collection frequency of accounting information and enables the administrative state for record collection type. Rerun: Y GSX Nav: N
Configure Telcordia Accounting	Defines the collection frequency of Telcordia mode accounting information and enables the administrative state for record collection type. All fields are mandatory. Rerun: Y GSX Nav: N
Configure RTCP	Configures RTCP interval values. Rerun: Y GSX Nav: N
Configure Performance Statistics	Configures performance statistic collection interval and interval size. Rerun: Y GSX Nav: N
Configure Policer System	Configures System Policer Rogue Media Grace Period, Set Threshold, Clear Threshold and State. Rerun: Y GSX Nav: N

Task Name	Task Description
Configure IP Application Access	Defines IP Application Access through Telnet, SSH, NTP, SNMP, FTP, NFS, and Port Mapper. Rerun: Y GSX Nav: N

Profiles

Task Name	Task description
Create DTMF Digit Profile	Creates a digit profile tailored to DTMF digit collection. Rerun: N GSX Nav: Y
Create MF Digit Profile	Creates a digit profile tailored to MF digit collection. Rerun: N GSX Nav: Y
Create Media Profile	Provides user defined DSP media profile configuration and management. Rerun: Y GSX Nav: Y
Create Packet Service Profile	Creates the named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: Y
Configure Packet Service Profile	Configures an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure Packet Service Profile Priority None	Configures no priority pertaining to audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure Packet Service Profile Priority G711/G711SS	Configures G711/G711SS priority pertaining to audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N

Task Name	Task description
Configure Packet Service Profile Priority G7231/G7231A	Configures G7231/G7231A priority for audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure Packet Service Profile Priority G726/G726SS	Configures G726/G726SS priority for audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure Packet Service Profile Priority G729A/G729AB	Configures G729A/G729AB priority for audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure Packet Service Profile Priority ILBC/ILBCSS	Configures ILBC/ILBCSS priority for audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: Y
Configure Packet Service Profile Priority G722/G722SS	Configures G722/G722SS priority pertaining to audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure Packet Service Profile Priority G7221/ G7221SS	Configures G722.1/G722.1SS priority pertaining to audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure Packet Service Profile Priority G728/G728SS	Configures G728/G728SS priority pertaining to audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure Packet Service Profile Priority AMR	Configures AMR priority pertaining to audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N

Task Name	Task description
Configure Packet Service Profile Priority AMRWB	Configures AMRWB priority pertaining to audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure Packet Service Profile Priority EFR	Configures EFR priority pertaining to audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure Packet Service Profile Priority EVRC	Configures EVRC priority pertaining to audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Create Pathcheck Ping Profile	Creates a Pathcheck ping profile including various timer and interval settings and used to verify continuity between an SBC 9000 and a peer SBC. Rerun: Y GSX Nav: Y
Create IKE Profile	Creates an Ike Profile by defining parameters such as the Encryption Cipher and the Lifetime. Rerun: Y GSX Nav: Y
Create Crank Back Profile	Defines call release codes that cause the GSX to attempt to reroute (or crankback) the call when a matching code is returned by Egress Signaling. Rerun: Y GSX Nav: N
Configure Crank Back Profile Add Reason	Create a Crank Back Profile and defines a call release code that causes the GSX to attempt to reroute (or crankback) the call when a matching code is returned by Egress Signaling. Rerun: Y GSX Nav: N
Create IPSec Profile	Creates an IP Sec Profile by defining parameters such as the Encryption Cipher and the Lifetime. Rerun: Y GSX Nav: Y

Task Name	Task description
Configure Packet Service Profile Priority Packet to Packet Control	Configures Packet To Packet Control for audio encoding for an existing named packet service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: Y
Create Circuit Service Profile	Creates the named circuit service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure Circuit Service Profile	Configures an existing named circuit service profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Create T1 Profile	Creates the named T1 profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Create T1 Profile with Thresholds Critical Create T1 Profile with Thresholds Major Create T1 Profile with Thresholds Minor	Creates the named T1 profile with parameters and threshold values provided and enables its administrative state. Rerun: Y GSX Nav: N
Create SCTP Profile	Creates a SCTP profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure T1 Profile TCA Filters	Profile defines T1 Threshold Crossing Alert (TCA) which is reported through an event log and trap. Rerun: Y GSX Nav: Y
Configure T1 Profile TCA Reports	Profile defines T1 Threshold Crossing Alert (TCA) reporting. Rerun: Y GSX Nav: Y
Create E1 Profile	Creates the named E1 profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N

Task Name	Task description
Create E1 Profile with Thresholds Critical Create E1 Profile with Thresholds Major Create E1 Profile with Thresholds Minor	Creates the named E1 profile with parameters and threshold values provided and enables its administrative state. Rerun: Y GSX Nav: N
Configure E1 Profile TCA Filters	Profile defines E1 Threshold Crossing Alert (TCA) which is reported through an event log and trap. Rerun: Y GSX Nav: Y
Configure E1 Profile TCA Reports	Profile defines E1 Threshold Crossing Alert (TCA) reporting. Rerun: Y GSX Nav: Y
Create Echo Canceller Profile	Creates the named Echo Canceller profile with parameters provided and enables its administrative state. Rerun: Y GSX Nav: N
Create Overload Profile	Specifies a set of congestion thresholds, congestion durations, and overload controls. Rerun: Y GSX Nav: N
Create Address Reachability Service Profile	Creates an Address Reachability Profile, including Blacklist and Recovery parameters, which the SBC 9000 uses to availability/ use of primary/secondary Application Servers. Rerun: Y GSX Nav: Y
Create Policer Discard Rate Profile	Creates/updates a Policer Discard Rate Profile with set and clear threshold and duration values for various parameters. If the provided profile name already exist, the system updates the existing profile with the provided values. Rerun: Y GSX Nav: N
Configure System Policer Alarm	Configures major and minor Policer Discard Rate Profiles. After configuring the profile, the corresponding mode is configured to InService. Rerun: Y GSX Nav: N

Task Name	Task description
Configure Server Policer Alarm	Configures major and minor Policer Discard Rate Profiles. After configuring the profile, the corresponding mode is configured to InService. Rerun: Y GSX Nav: N
Create High Probability of Completion Trunk Group Profile	Creates/updates a High Probability of Completion Trunk Group Profiles. If the provided profile name already exist, the system updates the existing profile with the provided values. Rerun: Y GSX Nav: Y
Create SIP Service Resource Priority Header Profile	Creates a SIP Service Resource Priority Header Profile. SIP Service Resource Priority Header Profile is also known as SIP Emergency Telecom Service Profile. Rerun: Y GSX Nav: Y
Create SIP Filter Profile	Creates a SIP Filter Profile. Rerun: Y GSX Nav: Y
Create SIP Transmit Profile	Creates a SIP Transmit Profile. Rerun: Y GSX Nav: Y
Create TLS Profile	Creates a TLS Profile. Rerun: Y GSX Nav: Y
Configure SIP Transmit Profile	Configures a SIP Transmit Profile. Rerun: Y GSX Nav: Y
Configure SIP Filter Profile	Configures an existing SIP Filter Profile. Rerun: Y GSX Nav: Y
Create SIP Adaptor Profile	Creates a SIP Adaptor Profile and adds a set of rules to it. It ignores an error message if a profile or rule already exists. You can create multiple profiles by repeating this task. Rerun: Y GSX Nav: N

Task Name	Task description
Add SIP Adaptor Profile Rule Criteria	Adds criteria to an existing rule. It first adds a criterion, then configures the criterion with the values specified. If the profile does not exist, an error message appears. You may ignore any error message that a criterion already exists. Rerun: Y GSX Nav: N
Add SIP Adaptor Profile Rule Action	Adds an action to an existing rule. It adds the action first and then configures the action with values specified. It ignores N error message if the action already exists, but it does not ignore error message of enabling profile state. You can add multiple actions to a profile by repeating this task. Rerun: Y GSX Nav: N
Enable SIP Adaptor Profile state	Enables the administrative state of multiple existing SIP adaptor profiles. Ideally, the state of an adaptor profile should be enabled in the add rule action task. But, an adaptor profile cannot be enabled until there are criteria and action(s) added and configured. You cannot enable the state in the Add Action task. Rerun: Y GSX Nav: N
Create SIP emergency profile	Creates SIP emergency profile Rerun: Y GSX Nav: Y
Create SIP Cause Mapping Profile	Creates a SIP cause mapping profile. Supports show, configure and delete operations. Rerun: Y GSX Nav: Y
Create SIP CAC Profile	Creates SIP CAC Profile Rerun: Y GSX Nav: Y
Create DBL Profile	Creates DBL Profile Rerun: Y GSX Nav: Y
Create MLPP TG Profile	Creates a Multilevel Precedence and Preemption Trunk Group Profile Rerun: Y GSX Nav: Y This is a licensed feature.

Task Name	Task description
Create SIP Service Option Tag Profile	Creates SIP Service Option Tag Profile. Rerun: Y GSX Nav: Y
Add DBL Profile Rule	Adds a rule to an existing DBL Profile. Rerun: Y GSX Nav: Y
Create SIP Service JIP Profile	Creates SIP Service JIP Profile. Defines the interworking of Jurisdiction information (JIP) between SIP and ISUP/SIP-I by sending JIP in the PAI/FROM/PDCS header. Rerun: Y GSX Nav: Y
Create SIP Service E164 Number Profile	Defines the rules for accomplishing local and global number conversions to E164 format before passing them to PSX for SIP. Rerun: Y GSX Nav: Y

Servers

This category of tasks provides a mechanism for creating server modules, some of which may be redundancy clients.

Refer to [GSX Installation Guide and Operations Guide](#) for a full discussion on server modules, redundancy groups, and redundancy clients. Management Server Modules are not defined using the task configurator.

Task Name	Task Description
Create Redundant Server	Creates a redundant Server and Adapter module pair in the indicated shelf and slot. Rerun: Y GSX Nav: Y

Task Name	Task Description
Create Server(s)/Redundancy Client(s)	Creates one or more modules with Server and Adapter module pairs in the indicated slot(s). You may create these server modules as clients of previously created redundant servers. If you specify the server a redundant client, the system creates its redundancy client group automatically and sets its administrative state to enabled. You may define more than one client module in a single task by specifying a contiguous range of slots. If there is a redundant module for this (these) client(s), select “Yes” in the Add to redundancy group field. You then have the option of either providing the redundant slot or the actual redundancy group name. In general, circuit clients should not specify the redundant slot or group name. Instead, specify the addition of these servers as clients to the redundancy group and the task determines the redundancy group name for you. This does not apply when adding CNS31 clients to CNS30 redundancy groups. In this case you should specify the redundancy group name (that is, CNS301). Packet (PNS10/20) clients should specify the slot number of the redundant server as defined above. Rerun: Y GSX Nav: Y
Enable Redundancy	Enables one or more redundancy groups after creating server modules on the chassis. A side effect of creating redundant modules is that the redundancy groups associated with them are automatically created and named. As you create client modules, the system automatically add them to these redundancy groups (as clients) during module creation. The last step in creating modules is to enable the redundancy groups. Redundancy group names for “1n” redundancy are named <serverhwtype><shelf> and group names for “11” redundancy are named <serverhwtype><shelf><redundant slot>. Redundancy group names for PNS10 and 20 modules are PNSxx<shelf><slot>. Redundancy group names for CNS10 and 30 modules are CNSxx<shelf>. Rerun: Y GSX Nav: N
Create Logical Bearer Address for Layer3 Redundancy Group with Mask	Creates a logical bearer address for Layer3 redundancy using a mask. Rerun: Y GSX Nav: N

Task Name	Task Description
Create Logical Bearer Address for Layer3 Redundancy Group with Size	Creates a logical bearer address for Layer3 redundancy using a size. Rerun: Y GSX Nav: N

OC3 Groups

This category of tasks provides for the creation and configuration of the OC3 subsystem.

Task Name	Task Description
Create OC3 Group	Creates an OC3 group on the slot specified and puts it in service. Rerun: Y GSX Nav: Y
Configure OC3 SONET Interface	Configures the SONET interface specified by the provided shelf, slot and port number. Rerun: Y GSX Nav: N
Configure OC3 SONET Path	Configures the specified sonet path on the shelf, slot and interface provided. You can specify a range of SONET paths with values 1 to 3. Rerun: Y GSX Nav: N
Configure OC3 SONET IF Thresholds	Configures thresholds on the specified SONET interface. Rerun: Y GSX Nav: N
Configure OC3 SONET Path Thresholds	Configures thresholds on the specified SONET path. You can specify a range of SONET paths with values 1 to 3. Rerun: Y GSX Nav: N
Configure OC3 APS	Configures the APS group (auto)created as part of the OC3 group creation. Rerun: Y GSX Nav: N

Events

This category of tasks provides for the configuration of several types of event filters.

Task Name	Task Description
Configure Accounting Event Log	Configures accounting event filtering for a particular shelf and slot. Rerun: Y GSX Nav: N

Task Name	Task Description
Configure Debug Event Log	Configures debug event filtering for a particular shelf and slot. Rerun: Y GSX Nav: N
Configure System Event Log	Configures system event filtering for a particular shelf and slot. Rerun: Y GSX Nav: N
Configure Trace Event Log	Configures trace event filtering for a particular shelf and slot. Rerun: Y GSX Nav: N
Configure Event Filter	Configures event filtering for a particular shelf and slot. Rerun: Y GSX Nav: N

System Timing

Task Name	Task Description
Create NTP Server	Creates and configures a reference to a system network timing protocol host on this chassis and enables its administrative state. Rerun: Y GSX Nav: N
Configure System Timing	Configures the system timing parameters on a particular shelf. Rerun: Y GSX Nav: N
Create System Timing Source	Creates and configures a system timing source for a particular management timing adapter and sets its administrative state to enabled. Rerun: Y GSX Nav: N
Configure System Timing Source	Configures a system timing source for a particular management timing adapter and sets its administrative state to enabled. The primary reason for this task is to alter the sequence number for an existing timing source. See “Resequence System Timing” below. Rerun: Y GSX Nav: N
Configure System Mgt Timing Adapter	Configures parameters for a particular management timing adapter for a shelf and enables its administrative state. Rerun: Y GSX Nav: N

Task Name	Task Description
Create Reference Clock Binding on Span	Configures a reference to a particular T1 span for a reference clock. Rerun: Y GSX Nav: N
Create Reference Clock Binding on CNS60	Configures a reference to a particular CNS60 port/span for a reference clock. Rerun: Y GSX Nav: N
Create Reference Clock Binding on OC12	Configures a reference to a particular OC12 for a reference clock. Rerun: Y GSX Nav: N
Create Reference Clock Binding on OC3	Configures a reference to a particular OC3 Slot for a reference clock. Rerun: Y GSX Nav: N
Create Reference Clock Binding on Pim Upper	Configures a reference to a particular PIM Slot as a reference clock into the MTA. Rerun: Y GSX Nav: N
Create Reference Clock Binding on Pim Lower	Configures a reference to a particular PIM Slot as a reference clock into the MTA. Rerun: Y GSX Nav: N
Resequence System Timing	Resequences the system timing for the specified shelf. Rerun: Y GSX Nav: N

Gateway to Gateway

Task Name	Task Description
Create Destination Gateway	Creates and configures a destination gateway for routing calls. This procedure automatically sets the gateway's admin state to enabled. Rerun: N GSX Nav: N

Task Name	Task Description
Create GW Signaling Port	Creates and configures a gateway signaling port. This procedure automatically sets the ports admin state to enabled and operational mode to in service. Reference port identifies the Gateway Signaling Port (1 for the first port, 2 for the optional second port). Rerun: Y GSX Nav: Y
Configure Gateway Signaling Link	Configures call timers for the gateways. Rerun: N GSX Nav: N

NIFs

This category of tasks provides for the configuration of existing Nif objects created and named during the creation of the server/adaptor module pairs (see [Servers](#)). These Nif procedures assume the default names.

When created, the system sets the admin state and operational mode of these Nifs to disabled and in service respectively. These Nif procedures do not assume the administrative state or operational mode of the Nifs prior to configuration and will take them out of service and disable them so that they may be configured. After successful configuration they will be administratively enabled and placed back into service.

Task Name	Task Description
Create NIF by Name	Creates an Ethernet port by specifying the name of the Nif. Rerun: Y GSX Nav: N
Configure Enet NIF by Port	Configures an existing Ethernet port. This procedure assumes the default Ether net Nif naming convention of ENET<shelf><slot><port>. The shelf, slot, and port values must be specified in order to construct this name. This procedure may be called regardless of the administrative state or operational mode of the Nif. Rerun: Y GSX Nav: N
Configure Gigabit Enet NIF by Port	Configures an existing Gigabit Ethernet port. This procedure assumes the default Gigabit Ethernet Nif naming convention of GENET<shelf><slot><port>. The shelf, slot, and port values must be specified in order to construct this name. This procedure may be called regardless of the administrative state or operational mode of the Nif. Rerun: Y GSX Nav: N

Task Name	Task Description
Configure Enet NIF by Name	Configures an existing Ethernet port by specifying the name of the Nif. This procedure may be called regardless of the administrative state or operational mode of the Nif. Rerun: Y GSX Nav: N
Configure Debug NIF	Configures a Debug Nif for a particular shelf and slot. Rerun: N GSX Nav: N
Create Gigabit Enet NIF SubInterface by NIF Port	Creates a Gigabit Enet Nif for a particular shelf (GSX9000 only) and slot. Rerun: N GSX Nav: N
Create NIF SubInterface by Name	Creates a NIF subinterface by specifying the name of the subinterface. You may call this procedure regardless of the administrative state or operational mode of the Nif. Rerun: Y GSX Nav: N
Create NIF Group and Add Interfaces/ SubInterfaces	Creates a NIF group if it does not exist, and add up to six each interfaces/subinterfaces to the NIF group. You may call this procedure regardless of the administrative state or operational mode of the Nif. Rerun: Y GSX Nav: N
Configure Ethernet IP Application Access	Configures access control to Ethernet IP applications through NIF Groups. Rerun: Y GSX Nav: Y
Configure Ethernet IPv6 Application Access	Configures access control to Ethernet IPv6 applications through NIF Groups. Rerun: Y GSX Nav: Y
Configure Ethernet Switch IP Address	Configures an ethernet switch address for a particular shelf and slot. Rerun: N GSX Nav: N

Task Name	Task Description
Create Port Redundancy Group	Creates Port Redundancy Group layer and port for a particular shelf and slot. Name, Shelf and Slot fields are mandatory. Rerun: N GSX Nav: N
Add Port to Port Redundancy Group	Add additional port to Port Redundancy Group. Name and Add Port fields are mandatory. Rerun: N GSX Nav: N
Create Link Detection Group	Create Link Detection Group. Name, Shelf, Slot and Thresholds fields are mandatory. Add Port is an optional field. Rerun: N GSX Nav: N
Add Port to Link Detection Group	Add additional port to the existing Link Detection Group. Name, Port fields are mandatory. Rerun: N GSX Nav: N
Configure Link Detection Group per Port	Configure Link Detection Group for a given port. All fields are mandatory. This procedure automatically sets the port's admin state to enabled after configuration. Rerun: N GSX Nav: N
Create Policer using NIF	Creates Policer using an existing NIF. Upon completion, this procedure automatically sets the Policer's admin state to enabled. Rerun: N GSX Nav: N
Create Policer using NIF Subinterface	Creates Policer using an existing NIF SubInterface. Upon completion, this procedure automatically sets the Policer's admin state to enabled. Rerun: N GSX Nav: N
Create Policer using MGMT NIF	Creates Policer using an existing MGMT NIF. Rerun: N GSX Nav: N
Create Policer using IPv6 MGMT NIF	Creates Policer using an existing IPv6 MGMT NIF. Rerun: N GSX Nav: N

Task Name	Task Description
Create Policer using IPv6 NIF Subinterface	Creates Policer using an existing IPv6 NIF SubInterface. Upon completion, this procedure automatically sets the Policer's admin state to enabled. Rerun: N GSX Nav: N
Create Policer using IPv6 NIF	Creates Policer using an existing IPv6 NIF. Upon completion, this procedure automatically sets the Policer's admin state to enabled. Rerun: N GSX Nav: N
Create Mirror Group	Creates Mirror Group. Rerun: N GSX Nav: N
Add Mirror Group interface	Adds a Mirror Group Interface to an existing Mirror Group. Rerun: N GSX Nav: N
Add Mirror Group subinterface	Adds a Mirror Group Sub-interface to an existing Mirror Group. Rerun: N GSX Nav: N

Optical Interfaces

Task Name	Task Descriptor
Configure Optical Interface	Configures the optical interface object. Rerun: N GSX Nav: Y
Configure APS	Configures Automatic Switching Protection. Rerun: N GSX Nav: N
Configure Optical Interface DS1s on 84 T1/63 E1 Spans	Configures the logical DS1 spans for an optical interface object. Rerun: N GSX Nav: N
Configure Optical Interface Path	Configures one or more paths for an optical interface object. Rerun: N GSX Nav: Y

Task Name	Task Descriptor
Configure Optical Interface Paths TCA Filters	Configures one or more Threshold Crossing Alerts (TCA) Filters for a path for an optical interface object. Rerun: Y GSX Nav: Y
Configure Optical Interface VT	Configures one or more virtual tributaries for an optical interface object. Rerun: N GSX Nav: Y
Configure Optical Interface Thresholds for all Lines	Configures thresholds for all lines for a optical interface object. Rerun: N GSX Nav: Y
Configure Optical Interface TCA Filters for all Lines	Configures one or more Threshold Crossing Alerts (TCA) Filters for all lines for an optical interface object. Rerun: Y GSX Nav: Y
Configure Optical Interface Thresholds for all Paths	Configures thresholds for all paths for a optical interface object. Rerun: N GSX Nav: Y
Configure Optical Interface Thresholds for all VTs	Configures thresholds for all virtual tributaries for a optical interface object. Rerun: N GSX Nav: Y
Configure Optical Interface VTs TCA Filters	Configures one or more Threshold Crossing Alerts (TCA) Filters for a range of VTS for an optical interface object. Rerun: Y GSX Nav: N
Configure Optical Interface Path TCA Filters	Configure Optical Interface Threshold Crossing Alerts (TCA) Filters for a specified path. Rerun: N GSX Nav: Y

OSPF

This category of tasks provides for the configuration of an OSPF instance on a GSX9000 MNS module. These steps are outlined here in the order that they must be performed. Refer to [GSX Operations Guide](#) for more detailed information about the CLI commands implemented by the Task Configurator.

Task Name	Task Description
Create OSPF	Creates an OSPF instance on the selected shelf. Rerun: N GSX Nav: N

Task Name	Task Description
Configure OSPF	Configures an existing OSPF area and type. Also, automatically sets the OSPF's admin state to enabled. Rerun: N GSX Nav: N
Enable OSPF	Enables OSPF on the specified shelf. Rerun: N GSX Nav: N
Configure OSPF Interface	Configures the IP addresses associated with OSPF interfaces. Also, automatically sets the OSPF's interface admin state to enabled. Rerun: N GSX Nav: N

OSPFV3

This category of tasks provides for the configuration of an OSPFV3 instance on a GSX9000 MNS module. These steps are outlined here in the order that they must be performed. Refer to [GSX Operations Guide](#) for more detailed information about the CLI commands implemented by the Task Configurator.

Task Name	Task Description
Configure OSPFV3	Configures an existing OSPFV3 area and type. Also, automatically sets the OSPF's admin state to enabled. Rerun:Y GSX Nav: Y
Create OSPFV3	Creates an OSPFV3 instance on the selected shelf. Rerun:Y GSX Nav: Y
Enable OSPFV3	Enables OSPFV3 on the specified shelf. Rerun:Y GSX Nav: Y
Create OSPFV3 Interface	Creates OSPFV3 interface. Rerun:Y GSX Nav: Y
Configure OSPFV3 Interface	Configures OSPFV3 interface. Rerun:Y GSX Nav: Y

ATM

This category of tasks provides for the configuration of an ATM network interface using similar steps outlined in the *GSX Operations Guide*. These steps are outlined here in the order that they must be performed.

Task Name	Task Description
Configure SONET Interface	Configures the SONET interface object which is automatically created when the PNS Server Module is created. The name of this SONET interface conforms to the following convention: SONET<shelf><slot>. The administrative state of the interface is automatically set to enabled. Rerun: Y GSX Nav: N
Configure ATM Interface	Configures the ATM Interface limits for the SONET interface. The port number must be 1. Rerun: N GSX Nav: N This task can not be rerun if there are active PVCs on this interface.
Create ATM NIF	Creates an additional ATM Nif object and sets its administrative state to enabled and operational state to in service. The port number must be 1. Rerun: N GSX Nav: N
Configure ATM NIF	Configures the existing ATM Nif object created and named when the appropriate server/ adapter module pairs are created (see Servers). This ATM Nif procedure assume the default ATM Nif naming convention. After successful configuration ATM Nif will be administratively enabled and placed back into service. The port number must be 1. Rerun: N GSX Nav: N
Configure ATM NIF by Name	Configures ATM Nif objects by name. This ATM Nif procedure does not assume the default ATM Nif naming convention. After successful configuration ATM Nif will be administratively enabled and placed back into service. Rerun: N GSX Nav: N

Task Name	Task Description
Create ATM Traffic Descriptor(s)	Creates a contiguous range of traffic descriptors and assigns a PVC cell rate to them by specifying starting descriptor and number of descriptors. Rerun: N GSXNav: N You can not rerun this task because once you create ATM Traffic Descriptors, they can not be modified.
Create ATM PVC	Creates an ATM PVC. Rerun: Y GSX Nav: N
Configure ATM Extension VC	Creates an ATMExtension Virtual Connection Network Interface and automatically enables it and places it in service. Rerun: N GSX Nav: N
Configure ATM APS	Identifies a redundant SONET network. Rerun: Y GSX Nav: N

Static Routes

This category of tasks provides for the definition of gateways that direct traffic from IP (Ethernet and ATM), Management, and Debug NIFs.

Task Name	Task Description
Create Nif Static Route	Defines a gateway for IP traffic. Rerun: N GSX Nav: N
Create Nif SubInterface Static Route	Defines a NIF subinterface static route. Rerun: N GSX Nav: N
Create IPv6 Nif Static Route	Creates IPv6 Nif static route. Rerun: N GSX Nav: N
Create Management Nif Static Route	Defines a gateway for Management traffic. Rerun: N GSX Nav: N

Task Name	Task Description
Create IPv6 Nif Subinterface Static Route	Defines IPv6 Nif Subinterface Static Route. Rerun: N GSX Nav: N
Create Debug Nif Static Route	Defines a gateway for Debug traffic. Rerun: N GSX Nav: N
Create IfIndex Static Route	Defines a IfIndex Static Route. Rerun: N GSX Nav: N
Create IF Index Static Route With IPv6	Defines IF index static route with IPv6. Rerun: N GSX Nav: N
Create Management IPv6 Nif Static Route	Defines management IPv6 Nif static route. Rerun: N GSX Nav: N

Circuits

This category of tasks provides for the configuration of existing circuit objects defined on the GSX.

The system automatically creates and names Circuit objects when it creates the server/adaptor module pairs (see [Servers](#)). These Circuit procedures assume these default names.

Task Name	Task Description
Configure T3(s)	Configures one or more T3 Circuits with the specified parameters. This procedure assumes the default naming convention of T3<shelf><slot> <t3index> where t3Index is set to 1. By specifying the starting and ending slots, you can configure a range of contiguous T3 cards. This procedure automatically configures the T3(s) as enabled and in service. A partial description of the fields on this screen follows: Shelf defaults to 1 Slot Start the first slot containing the T3 object(s) Slot End the last slot containing the T3 object(s) Rerun: N GSX Nav: N

Task Name	Task Description
Configure T1(s) on T3	Configures one or more T1 Circuits on a T3 with the specified parameters. This procedure assumes the default naming convention of T1<shelf><slot> <ds3index> where t3Index is set to 1. By specifying the starting and ending slots, you can configure a range of contiguous T1 cards. By default, the system configures all 28 spans. This procedure automatically configures the T1 Spans as enabled and in service. A partial description of the fields on this screen follows: Shelf defaults to 1 Slot Start the first slot containing the T3 object(s) Slot End the last slot containing the T3 object(s) Span Start the starting span every T1 object being configured. Span End the ending span for every T1 object being configured. Rerun: N GSX Nav: N
Configure T1(s) on T3 using Profile	Similar to Configure T1(s) on T3 except that the system uses a profile to configure the T1(s) rather than specified parameters. By specifying the starting and ending slots, you can configure a range of contiguous T1 cards. By default, the system configures all 28 spans. This procedure automatically configures the T1 Spans as enabled and in service. A partial description of the fields on this screen follows: Shelf defaults to 1 Slot Start the first slot containing the T3 object(s) Slot End the last slot containing the T3 object(s) Span Start the starting span every T1 object being configured. Span End the ending span for every T1 object being configured. Rerun: N GSX Nav: N

Task Name	Task Description
Configure 12/36 Spans T1(s)	Configures one or more T1 Circuits with the specified parameters. This procedure assumes the default naming convention of T1<shelf><slot> By specifying the starting and ending slots, you can configure a range of contiguous T1 cards. By default, the system configures all 12/36 spans. This procedure automatically configures the T1 Spans as enabled and in service. A partial description of the fields on this screen follows: Slot Start the first slot containing the T1 object(s) Slot End the last slot containing the T1 object(s) Span Start the starting span every T1 object being configured. Span End the ending span for every T1 object being configured. Rerun: N GSX Nav: N
Configure 12/36 Spans T1(s) using Profile	Similar to Configure T1(s) except that the system uses a profile to configure the T1 spans rather than the specified parameters. This procedure automatically configures the T1 Spans as enabled and in service. By default, the system configures all 12/36 spans. A partial description of the fields on this screen follows: Slot Start the first slot containing the T1 object(s) Slot End the last slot containing the T1 object(s) Span Start the starting span every T1 object being configured. Span End the ending span for every T1 object being configured. Rerun: N GSX Nav: N

Task Name	Task Description
Configure 84 Spans T1(s)	Configures one or more T1 Circuits with the specified parameters. This procedure assumes the default naming convention of T1<shelf><slot> By specifying the starting and ending slots, you can configure a range of contiguous T1 cards. This procedure automatically configures the T1 Spans as enabled and in service. A partial description of the fields on this screen follows: Shelf defaults to 1. Slot Start the first slot containing the T1 object(s) Slot End the last slot containing the T1 object(s) Span Start the starting span of every T1 object being configured. Span End the ending span of every T1 object being configured. Rerun: N GSX Nav: N
Configure 84 Spans T1(s) using Profile	Similar to Configure T1(s) except that the system uses a profile to configure the T1 spans (up to 84) rather than the specified parameters. This procedure automatically configures the T1 Spans as enabled and in service. A partial description of the fields on this screen follows: Shelf defaults to 1. Slot Start the first slot containing the T1 object(s) Slot End the last slot containing the T1 object(s) Span Start the starting span of every T1 object being configured. Span End the ending span of every T1 object being configured. Rerun: N GSX Nav: N

Task Name	Task Description
Configure 8 Span E1(s)	Configures one or more 8 Span E1 Circuits with the specified parameters. This procedure assumes the default naming convention of E1<shelf><slot>. By specifying the starting and ending slots, you can configure a range of contiguous E1 cards. By default, the system configures all 8 spans. This procedure automatically configures the E1 Spans as enabled and in service. A partial description of the fields on this screen follows: Slot Start the first slot containing the E1 object(s) Slot End the last slot containing the E1 object(s) Span Start the starting span every E1 object being configured. Span End the ending span for every E1 object being configured. Rerun: N GSX Nav: N
Configure 8 Span E1(s) using Profile	Similar to Configure 8 Span E1(s) except that the system uses a profile to configure the E1 spans rather than the specified parameters. By specifying the starting and ending slots, you can configure a range of contiguous E1 cards. By default, the system configures all 8 spans. This procedure automatically configures the E1 Spans as enabled and in service. A partial description of the fields on this screen follows: Slot Start the first slot containing the E1 object(s) Slot End the last slot containing the E1 object(s) Span Start the starting span every E1 object being configured. Span End the ending span for every E1 object being configured. Rerun: N GSX Nav: N

Task Name	Task Description
Configure 12/36 Span E1(s)	Configures one or more 12/36 Span E1 Circuits with the specified parameters. This procedure assumes the default naming convention of E1<shelf><slot>. By specifying the starting and ending slots, you can configure a range of contiguous E1 cards. By default, the system configures all 12/36 spans. This procedure automatically configures the E1 Spans as enabled and in service. A partial description of the fields on this screen follows: Slot Start the first slot containing the E1 object(s) Slot End the last slot containing the E1 object(s) Span Start the starting span for every E1 object being configured. Span End the ending span for every E1 object being configured. Rerun: N GSX Nav: N
Configure 12/36 Span E1(s) using Profile	Similar to Configure 12/36 Span E1(s) except that the system uses a profile to configure the E1 spans rather than the specified parameters. By specifying the starting and ending slots, you can configure a range of contiguous E1 cards. By default, the system configures all 12/36 spans. This procedure automatically configures the E1 Spans as enabled and in service. A partial description of the fields on this screen follows: Slot Start the first slot containing the E1 object(s) Slot End the last slot containing the E1 object(s) Span Start the starting span every E1 object being configured. Span End the ending span for every E1 object being configured. Rerun: N GSX Nav: N

Task Name	Task Description
Configure 63 Span E1(s)	Configures one or more 63 Span E1 Circuits with the specified parameters. This procedure assumes the default naming convention of E1<shelf><slot>. By specifying the starting and ending slots, you can configure a range of contiguous E1 cards. This procedure automatically configures the E1 Spans as enabled and in service. A partial description of the fields on this screen follows: Slot Start the first slot containing the E1 object(s) Slot End the last slot containing the E1 object(s) Span Start the starting span of every E1 object being configured. Span End the ending span of every E1 object being configured. Rerun: N GSX Nav: N
Configure 63 Span E1(s) using Profile	Similar to Configure 12 Span E1(s) except that the system uses a profile to configure the E1 spans rather than the specified parameters. By specifying the starting and ending slots, you can configure a range of contiguous E1 cards. This procedure automatically configures the E1 Spans as enabled and in service. A partial description of the fields on this screen follows: Slot Start the first slot containing the E1 object(s) Slot End the last slot containing the E1 object(s) Span Start the starting span of every E1 object being configured. Span End the ending span of every E1 object being configured. Rerun: N GSX Nav: N

Ribbon Softswitch

Note

For purposes of this topic, the Softswitch task uses "Sonus Soft Switch" terminology.

Task Name	Task Description
Configure Sonus Soft Switch Global Settings	Configures the Ribbon Softswitch switchover and retry settings. Rerun: Y GSX Nav: N
Create Sonus Soft Switch	Creates a reference to a Ribbon Softswitch on the GSX. This procedure automatically sets the reference to the soft switch as enabled and in service. Rerun: Y GSX Nav: N

MGCP

This category of tasks provides for the configuration of MGCP and IUA objects.

Task Name	Task Description
Configure MGCP Gateway	Configures MGCP gateway. Rerun: N GSX Nav: N
Create MGCP Service Profile	Creates MGCP service profile. Rerun: N GSX Nav: N
Create MGCP Session	Creates MGCP session. Rerun: N GSX Nav: N
Create MGCP Call Agent	Creates MGCP call agent. Rerun: N GSX Nav: N
Create MGCP IPv4 Connection	Creates MGCP IPv4 connection. Rerun: N GSX Nav: N

H323

This category of tasks provides for the configuration of H.323.

Task Name	Task Description
Create Zone	Creates an H.323 zone, which you can use to group sets of H.323 signaling ports and service groups. Rerun: Y GSX Nav: Y
Configure H323 Signaling Timers	Configures H323 Signaling Timer. Rerun: Y GSX Nav: Y
Configure H323 Signaling Port for H225	Configures H323 Signaling Port for H225. Rerun: Y GSX Nav: Y
Configure H323 Signaling Port for H245	Configures H323 Signaling Port for H245. Rerun: Y GSX Nav: Y
Configure Mode for H323 Signaling Port	Configures the H323 signaling service operational state. The modes can be In Service or Out of Service. In Service - The signaling port listens for incoming H323 signal link connection requests. Out of Service - The signaling port is not available for incoming H323 signal link connection requests and thus cannot be used to create new gateway signal links to other H323 gateways. Rerun: Y GSX Nav: Y
Configure Action for H323 Signaling Port	Specifies the method by which the active calls using this H323 signaling service are processed when Mode goes to out-of-service. Rerun: Y GSX Nav: Y
Configure Action Timeout for H323 Signaling Port	The time (in minutes) to wait for active calls to finish in order to place the H323 signaling service in out-of-service Mode. Rerun: Y GSX Nav: Y

SIP

This category of tasks provides for the configuration of SIP.

Task Name	Task Description
Create Zone	Creates an SIP zone, which you can use to group sets of SIP signaling ports and service groups. Rerun: Y GSX Nav: Y

Task Name	Task Description
Create DNS Server	Creates a SIP DNS Server with the specified Server Name and IP Address. Rerun: Y GSX Nav: Y
Create IPv6 DNS Server	Creates a IPv6 SIP DNS Server with the specified Server Name and IP Address. Rerun: Y GSX Nav: Y
Create SIP Signaling Port on Mgt or PNA NIF	Creates a SIP signalling port with the specified port and IP Address.The GSX listens for SIP signalling on this IP Address and port number. The Role can be primary or secondary. Rerun: N GSX Nav: N
Create SIP Signaling Port on Mgt or PNA NIF with IPv6	Creates a SIP signalling port with the specified port and IPv6 Address.The GSX listens for SIP signalling on this IP Address and port number. The Role can be primary or secondary. Rerun: N GSX Nav: N
Configure SIP Signaling Controls	Establishes certain SIP Signaling Control parameters including maximum PDU size, loopback detection on incoming INVITES and the maintenance of per dialog/transaction statistics for basic SIP responses and requests for completed calls/ transactions. Rerun: N GSX Nav: N
Add SIP ACLs	Sets up an access control list for the Application Server. Rerun: N GSX Nav: N
Configure SIP Signaling Registration	Define SIP Signaling Registration parameters. Rerun: N GSX Nav: N
Create SIP to CPC Cause Mapping Profile	Creates a SIP to CPC cause code mapping profile based on default CauseMap Profile, assigns a unique profile identifier and defines parameter values where applicable. Rerun: Y GSX Nav: N
Add SIP Cause to SIP to CPC Mapping Profile	Adds a SIP cause that does not exist to the named SIP to CPC mapping profile. Rerun: Y GSX Nav: N

Task Name	Task Description
Create CPC to SIP Cause Mapping Profile	Creates a CPC to SIP cause code mapping profile based on default CauseMap Profile, assigns a unique profile identifier and defines (Unrec Action) value. Rerun: Y GSX Nav: N
Add CPC Cause to CPC to SIP Mapping Profile	Add a CPC cause that does not exist to the named CPC to SIP mapping profile. Rerun: Y GSX Nav: N
Create SIP Peer	Creates a SIP peer. Rerun: Y GSX Nav: N

Media Gateway

This category of tasks provides for the configuration of a Media Gateway.

Task Name	Task Description
Create Media Gateway Service	Creates a media gateway service. Rerun: N GSX Nav: N
Create Media Gateway Circuits	Creates media gateway circuits. Rerun: N GSX Nav: N
Create Media Gateway Circuits on T1(s) on T3	Creates media gateway circuits for T1's on a T3. Rerun: N GSX Nav: N
Create Media Gateway Circuits on T1(s)	Creates media gateway circuits for T1's. Rerun: N GSX Nav: N
Create Media Gateway Circuits on CNS60	Creates media gateway circuits on a CNS60 card. Rerun: N GSX Nav: N
Create Media Gateway Circuits on CNS71/81/86	Creates media gateway circuits on a CNS71/81/86 card. Rerun: N GSX Nav: N
Create Media Gateway Interface	This object defines the GSX hardware, and the NIFGROUP/VLAN_ID pair (or pairs) that will support a physical IP termination (IpTerm), on behalf of the Media Gateway Border Gateway Function. Rerun: Y GSX Nav: Y

Task Name	Task Description
Configure Media Gateway Interface Set VLAN/NIF Group	This object configures the NIFGROUP/VLAN_ID pair (or pairs) that will support a physical IP termination (IpPterm) on behalf of the Media Gateway Border Gateway Function. Rerun: N GSX Nav: N
Create Media Gateway Circuits on 8 Span E1(s)	Creates media gateway circuits for 8 Span E1's. Rerun: N GSX Nav: N
Create Media Gateway Circuits on 12 Span E1(s)	Creates media gateway circuits for 12 Span E1's. Rerun: N GSX Nav: N

SS7 Gateway

Task Name	Task Description
Create SS7 MPT2 Link Profile	Creates and configures an SS7 MTP2 Link Profile. Rerun: Y GSX Nav: N
Create SS7 MPT3 ANSI Profile	Creates and configures an SS7 MTP3 ANSI Profile. Rerun: Y GSX Nav: N
Create SS7 MPT2 Link	Creates and configures an SS7 MTP2 Link. Rerun: Y GSX Nav: N
Create SS7 MPT3 ITU Profile	Creates and configures an SS7 MTP3 ITU Profile. Rerun: Y GSX Nav: N
Create SS7 MPT3 ANSIMGMT	Creates and configures an SS7 MTP3 ANSIMGMT object. Rerun: Y GSX Nav: N
Create SS7 MPT3 ITUMGMT	Creates and configures an SS7 MTP3 ITUMGMT object. Rerun: Y GSX Nav: N

Task Name	Task Description
Create SS7 Gateway for DGMS Type	Creates and configures an SS7 Gateway with primary and secondary links. The secondary host is optional. The gateway type is configured to dgms. This procedure automatically sets the administrative state and operational mode for the primary and secondary (if specified) to enabled and in service respectively. Rerun: Y GSX Nav: Y
Create SS7 Gateway for M3UA Type	Creates and configures an SS7 Gateway with primary and secondary links. The secondary host is optional. The gateway type is configured to m3ua. This procedure automatically sets the administrative state and operational mode for the primary and secondary (if specified) to enabled and in service respectively. Rerun: Y GSX Nav: Y
Create SS7 Node	Creates and configures an SS7 Node and assigns it to an SS7 Gateway. This task automatically sets the SS7 Nodes admin state to enabled and operational state to in service. A partial description of the fields on this screen follows: Local PC The local or originating point code that identifies the SS7 node, must comply the point code format with respect to the protocol type shown below. Protocol Type ANSI, BT7, China, ETSI, ITU, or JAPAN. SS7 Node Profile If provided, the system obtains the point code size and point code format from the SS7 Node Profile. Point Code Size The point code sizes (bits). Supported are: 24 for ANSI, 14 for ITU, and 16 for JAPAN. Entries in this field override the point code size specified in the SS7 Node Profile. Point Code Format The point code formats supported are: 888 (bits) for ANSI, 383 for ITU and BTIUP, and 457 for JAPAN. You may enter the information in decimal format: 24 for ANSI, 14 for ITU and BTIUP, and 16 for JAPAN. Entries in this field override the point code format specified in the SS7 Node Profile. Rerun: Y GSX Nav: Y

Task Name	Task Description
Create SS7 Node Without Gateway	Creates and configures an SS7 Node without assigning it to a Gateway. Rerun: Y GSX Nav: N
Configure SS7 Node Timers	Configures the timers for an existing SS7 Node. Rerun: Y GSX Nav: Y
Create SS7 Destination	Creates and configures an SS7 Destination object. Rerun: Y GSX Nav: N
Create SS7 Link	Creates and configures an SS7 Link object. Rerun: Y GSX Nav: N
Create SS7 Link Set	Creates and configures an SS7 Link Set object. Rerun: Y GSX Nav: N
Create SS7 Route	Creates and configures an SS7 Route object. Rerun: Y GSX Nav: N

Common Provisioning

This category of tasks provides for the configuration of Carrier Codes, Disconnect SSPs and Treatment Profiles, Tone Profiles, and Tone Types and Tone Packages. You may also create and use these objects in ISUP, ISDN, and CAS tasks.

Task Name	Task Description
Create Carrier	Creates and configures a carrier code and name. Also, automatically sets the carrier codes administrative state to enabled. Rerun: N GSX Nav: N
Create Disconnect Signaling Sequence (SSP)	Creates a CAS signaling sequence profile and adds a new token to the profile. If the profile already exists, the system adds the token and its parameters to the sequence at the specified position. Rerun: N GSX Nav: Y

Task Name	Task Description
Create Disconnect Signaling Sequence (SSP) Table	Creates one or more CAS signaling sequence profile and adds a new token to the profile. If the profile already exists, the token and its parameters are added to the sequence at the specified position. You can create up to 32 entries. The sequence position and the two parameter fields are optional. Rerun: N GSX Nav: Y
Create Disconnect Treatment Profile	Assigns a disconnect treatment reason code to an existing signaling sequence profile. Rerun: N GSX Nav: Y
Create Single Frequency Tone Profile	Creates and configures a single frequency tone profile. Rerun: N GSX Nav: Y
Create Dual Frequency Tone Profile	Creates and configures a dual frequency tone profile. Rerun: N GSX Nav: Y
Create Amplitude Modulated Tone Profile	Creates and configures an amplitude modulated tone profile. Rerun: N GSX Nav: Y
Create Composite Tone Profile	Creates and configures a composite tone profile. The profile defines the parameters to generate call progress tones. Rerun: N GSX Nav: Y
Create Tone Type	Creates a tone type whose name can be assigned to a tone profile in a tone pack age. Rerun: N GSX Nav: Y
Create Tone Package	Creates a tone package and assigns a tone type / tone profile name pair to the package. If the tone package already exists, the system adds the name pairs to the package. Rerun: N GSX Nav: Y

Task Name	Task Description
Create Trunk Group Profile	Creates a trunk group profile. If used as a trunk group profile for ISUP, the SS7 node name must be provided. This task automatically sets the profiles admin state to enabled. Rerun: Y GSX Nav: Y

LP (Local Policy) Provisioning

This category of tasks provides for the creation/configuration of object related to the Local Policy function on the GSX, including Dial Plans, Standard Routes, Routing Labels, and Signaling Profiles.

Task Name	Task Description
Create Dial Plan	This object creates and configures a DIAL PLAN used for Number and call type analysis on the GSX in Local Policy mode for Input Call Processing. The interface includes the following parameters: • Plan Name the name of the dial plan to be created. • National Access Code the national access code the plan to use. • International Access Code the international access code the plan to use. • Operator Number the operator's number for the plan. Rerun: Y GSX Nav: N
Create IP Signaling Peer	Creates and configures an IP signaling peer. This procedure creates and configures a new IP signaling Peer. If the signaling peer already exists, it configures it. • IP Signaling Peer Name the name of the IP signaling peer to be created. • IP Address the IP address the signaling peer to use. • Port the port the signaling peer to use. • FQDN the FQDN the signaling peer to use. • Zone the Zone the signaling peer to use. Rerun: Y GSX Nav: N
Create IP Signaling Profile	Creates and configures an IP signaling profile. This procedure creates and configures a new IP signaling Profile. If the signaling profile already exists, it configures it. Rerun: Y GSX Nav: N

Task Name	Task Description
Configure IP Signaling Profile	Configures an IP signaling profile. This procedure configures a existing IP signaling Profile. Rerun: Y GSX Nav: Y
Create Signaling Profile	Creates and configures a signaling profile. This procedure creates and configures a new signaling profile. If the signaling profile already exists, it configures it. • Profile Name the name of the signaling profile to be created. • Ingress Don't Generate Exit Message flag for not generating exit message. • Ingress Propagate FE Parameter flag for propagating FE parameter. • Egress Convert Number to E164 Format flag for converting number to E164 format. Rerun: Y GSX Nav: N
Configure Signaling Profile	This procedure configures a signaling profile. • Profile Name the name of the signaling profile to be created. • Ingress Don't Generate Exit Message flag for not generating exit message. • Ingress Propagate FE Parameter flag for propagating FE parameter. • Egress Convert Number to E164 Format flag for converting number to E164 format. Rerun: Y GSX Nav: N

Task Name	Task Description
Create Routing Label	This procedure creates and configures a new routing label. If the routing label already exists, it configures it. • Label Name the name of the routing label to be created. • Primary PSTN Trunk Group the primary PSTN trunk group to use. • Primary IP Signaling Peer the primary IP signaling peer to use. • Primary Route Type the primary routing type. • Primary State the admin state for primary routing. • Secondary PSTN Trunk Group the secondary PSTN trunk group to use. • Secondary IP Signaling Peer the secondary IP signaling peer to use. • Secondary Route Type the secondary routing type. • Secondary State the admin state for secondary routing. Rerun: Y GSX Nav: N
Configure Routing Label	This procedure configures a routing label. • Label Name the name of the routing label to be created. • Primary PSTN Trunk Group the primary PSTN trunk group to use. • Primary IP Signaling Peer the primary IP signaling peer to use. • Primary Route Type the primary routing type. • Primary State the admin state for primary routing. • Secondary PSTN Trunk Group the secondary PSTN trunk group to use. • Secondary IP Signaling Peer the secondary IP signaling peer to use. • Secondary Route Type the secondary routing type. • Secondary State the admin state for secondary routing. Rerun: Y GSX Nav: N
Create Standard Route	This procedure creates and configures a new standard route. If the standard route already exists, it configures it. • Routing Label the routing label to use. • Source Trunk Group the source trunk group to use. • Destination Number Prefix the prefix for destination number. Rerun: N GSX Nav: N

Task Name	Task Description
Create Local Policy Trunk Group Profile	This procedure creates and configures a new local policy trunk group profile. If the profile already exists, it configures it. • Profile Name the name of profile to be created. • Signaling Profile Name the name of signaling profile to use. • Signaling Flag the Signaling flag to use. • IP Signaling Profile Name the name of IP signaling profile to use. • Packet Service Profile Name the name of packet service profile to use. • Dial Plan the dial plan to use. • Country Code the country code to use. • Destination Switch Type the type of destination switch. Rerun: N GSX Nav: N
Configure Local Policy Trunk Group Profile	This procedure configures a local policy trunk group profile. • Profile Name the name of profile to be created. • Signaling Profile Name the name of signaling profile to use. • Signaling Flag the Signaling flag to use. • IP Signaling Profile Name the name of IP signaling profile to use. • Packet Service Profile Name the name of packet service profile to use. • Dial Plan the dial plan to use. • Country Code the country code to use. Destination Switch Type the type of destination switch. Rerun: N GSX Nav: N
Configure Directory Service	This procedure configures the directory service. Rerun: N GSX Nav: Y
Create Tone Announcement Profile	Creates a new tone announcement profile. Rerun: Y GSX Nav: Y
Create Translation Label	Creates new translation labels to support ENUM query. Rerun: Y GSX Nav: Y
Create Translation Entry	Creates a new translation entry Rerun: Y GSX Nav: Y

ISUP Provisioning

This category of tasks provides for the configuration of SS7 Gateways, SS7 Nodes, Trunk Groups, ISUP Services and ISUP Circuit objects.

Many ISUP provisioning tasks include the **Stop if element exists** field. When set to **Yes** (the default), this setting stops the task from executing if a GSX object with the specified name already exists. This prevents existing GSX entries (such as inservice Trunk Groups) from being inadvertently overwritten when new objects are provisioned. When set to No, the task executes without checking for previously-defined element names.

Task Name	Task Description
Create ISUP Trunk Group Profile	Creates a trunk group profile and assigns it to existing carrier code and SS7 Node name references. Also, automatically sets the profiles admin state to enabled. Both the carrier code and the SS7 Node references must exist on the GSX9000 before calling this task. Rerun: Y GSX Nav: Y
Create ISUP Trunk Group	Creates a trunk group and assigns it a carrier code and SS7 Node reference. Also, automatically sets the trunk group admin state to enabled. Both the carrier code and the SS7 Node references must exist on the GSX9000 before calling this task. Rerun: N GSX Nav: Y
Create BICC Trunk Group	Creates a BICC trunk group and assigns it a carrier code and SS7 Node reference. Also, automatically sets the trunk group admin state to enabled. Both the carrier code and the SS7 Node references must exist on the GSX9000 before calling this task. Rerun: N GSX Nav: Y
Create ISUP Trunk Group using Profile	Creates a trunk group with parameters obtained from the references trunk group profile. Also, automatically sets the trunk group admin state to enabled. The trunk group profile must exist on the GSX9000 before calling this task. Rerun: N GSX Nav: Y

Task Name	Task Description
Create ISUP Trunk Groups	Creates a trunk group for every unique span indicated across one or more slots. The naming convention follows that of the default naming convention of circuit objects, except that the name prefix will be used. A partial description of the fields on this screen follows: Name Prefix the prefix to use when generating trunk group names. Shelf defaults to 1. Slot Start the starting slot for creating the trunk groups. Slot End the ending slot for creating the trunk groups. DS3 Index indicates whether the trunk group naming convention should follow those of a real T1 or that of T1's on a T3. If the DS3 index is 0, the names of the trunk group will follow: <nameprefix><shelf><slot>; otherwise, it will follow: <nameprefix><shelf><slot><ds3 index>. Span Start the starting span for every slot specified by the range of slot start to end. Span End the ending span for every slot specified by the range of slot start to end. The number of trunk groups created is determined as follows: (slot end slot start) * (span end span start) Rerun: N GSX Nav: N
Create ISUP Trunk Groups using Profile	The same as "Create ISUP Trunk Groups" except that a trunk group profile is used exclusively to provide configuration settings for the created trunk groups. Rerun: N GSX Nav: N

Task Name	Task Description
Create ISUP Signaling Profile	Creates an ISUP signaling profile. Also, automatically sets the profiles admin state to enabled. Rerun: N GSX Nav: Y A new parameter LOG CHARGE INFO FROM ITX IN CDR is added. The parameter specifies whether to log the aggregate value of charge units received in ITX message in intermediate and stop the CDR records. By default the parameter value is unsupported. If supported, then it will log the aggregate value of charge units received in ITX message in intermediate and stop CDR records, in ISUP-ISUP, SIPI-SIPI, ISUP-SIPI, SIPI-ISUP call scenario.
Create ISUP Signaling Group	The ISUP signaling group gives the ISUP library all required information for the purposes of encoding or decoding the message. Also, automatically sets the signaling group admin state to enabled. Rerun: Y GSX Nav: Y
Create ISUP Information Request Profile	Creates an ISUP information request profile to be used by an ISUP service profile. This task automatically sets the profiles admin state to enabled. Rerun: N GSX Nav: Y
Create ISUP Service Profile	Creates an ISUP service profile that references an existing trunk group profile. Also, automatically sets the profiles admin state to enabled. The trunk group profile must exist on the GSX9000 before calling this task. Rerun: N GSX Nav: Y

Task Name	Task Description
Create ISUP Service	Creates and configures an ISUP service group with references to a trunk group and service profile. This task automatically sets the service groups admin state to enabled and operational state to in service. The trunk group and service profile (if provided) references must exist on the GSX9000 before calling this task. SGX Configuration (Create CC Client) • Automatically Configure SGX: This determines if automatic SGX configuration will be performed or not • Dual CE: Yes, if dual CE is in use, otherwise No • (MNS1) Host Name 1: DNS name for GSX IP address 1 • (MNS1) Alternate Host Name 1: DNS name for GSX IP address 2 • (MNS2) Host Name 2: DNS name for GSX IP address 3 • (MNS2) Alternate Host Name 2: DNS name for GSX IP address 4 • Point Code Format: Format of the Destination Point Code previously entered. Rerun: N GSX Nav: Y
Create ISUP Circuits	Creates one or more ISUP Circuits (CIC's) associated with an ISUP Service Group and assigns them to channels on one or more Ports (Spans). This task automatically sets the admin state to enabled and operational state to in service for all circuits created. A full description of the fields on this screen follows: Shelf defaults to 1 Slot the slot associated with the server module containing the channels associated with CICs. DS3 Index the index associated with the DS3 used in forming the names of the spans. If creating circuits on a T1 card, set this parameter to 0. If creating circuits on a T3 card, set this parameter to 1. The default setting is 1. ISUP Service Name the named reference to an existing ISUP Service Group. Circuit Service Profile the named reference to an existing circuit service profile. Span Start the starting span for circuit assignment. This

Task Name	Task Description
	parameter defaults to 1. Span End the ending span for circuit assignment. Maximum values are: 28 (for a T1 on a T3), or 12 for a T1. The default setting is 28. Channel Start the starting channel number for the circuit assignment process for each specified span. The system uses this parameter in conjunction with the CICs per Port parameter (specified below) to determine the contiguous range of channels associated with the CICs. This range is identical for all Spans. This parameter defaults to 1. CIC Start the starting CIC number for the entire assignment process. CICs per Port The number of CICs assigned to channels on each Port (Span). The maximum is 24. By default, this task creates CICs across all T1 spans within a T3. If you are provisioning a T1 card (cns10/cna10 server/adaptor pair), set the DS3 Index to 0 and Num Ports to a maximum of 12. The number of CICs created and assigned to channels is equal to: Num Ports * CICs per Port The contiguous range of channels used across all specified Ports is equal to: CIC Start to CICs per Port Rerun: N GSX Nav: Y
Create ISUP Circuits on T1 on T3	Identical to "Create ISUP Circuits" except that this task is tailored to CIC assignment across T1 Spans on a T3 (up to 28 spans x 24 CICs per span). Rerun: N GSX Nav: Y
Create ISUP Circuits on T1	Identical to "Create ISUP Circuits" except that this task is tailored to CIC assignment across T1 Spans on a T1 (up to 12 spans x 24 CICs per span). Rerun: N GSX Nav: Y
Create ISUP Circuits on 3xT3 CNS60/80/85	Identical to "Create ISUP Circuits" except that this task is tailored to CIC assignment across Spans on a CNS60/80/85 card (up to 3 x 28 spans x 24 CICs per span). Rerun: N GSX Nav: Y

Task Name	Task Description
Create ISUP Circuits on 84 T1/ 63 E1 Spans	Identical to "Create ISUP Circuits" except that this task is tailored to CIC assignment across Spans on a CNS71/81/86 card (up to 84 spans x 24 CICs per span). Rerun: N GSX Nav: Y
Create ISUP Circuits on an 8 Span E1	Identical to "Create ISUP Circuits" except that this task is tailored to CIC assignment across E1 Spans (up to 8 spans x 31 CICs per span). Rerun: N GSX Nav: Y
Create ISUP Circuits on a 12/ 36 Span E1	Identical to "Create ISUP Circuits" except that this task is tailored to CIC assignment across E1 Spans (up to 12/36 spans x 31 CICs per span). Rerun: N GSX Nav: Y
Create ISUP Circuits across Slots	Identical to "Create ISUP Circuits" except that it assigns CICs across multiple Slots. Its default values are tailored towards a T1. Fields added to this task are: Slot Start the starting slot for assignment. Slot End the ending slot for assignment. Rerun: N GSX Nav: Y

Task Name	Task Description
Create ISUP Circuits By Handling Group	Creates ISUP Circuits (CIC's) associated with an ISUP Service Group and assigns them to channels on one or more Ports (Spans). The assignments follow a rule that is unique to Japan that skips 4 channels for each increment in CIC value. This task automatically sets the admin state to enabled and operational state to in service for all circuits created. A full description of the fields on this screen follows: Shelf (GSX9000 only) defaults to 1. Slot (GSX9000 only) the slot associated with the server module whose channels will be associated with CICs. DS3 Index (GSX9000 only) Indicates whether the T1's are on a T3. If creating circuits on a T1 card, this parameter should be 0. If creating circuits on a T3 card, this parameter should be 1. The default setting is 1. ISUP Service Name The named reference to an existing ISUP Service Group. Circuit Service Profile The named reference to an existing circuit service profile. This parameter is optional. Port Start (GSX9000) The port to begin circuit assignment at. This parameter defaults to 1. Span Start (GSX9000 only) The span to begin circuit assignment at. This parameter defaults to 1. Number of Spans (GSX9000 only) Number of spans to assign circuits on. This parameter can be as high as 28 (for a T1 on a T3) or as high as 12 for a T1. The default setting is 28. CIC Start The starting CIC number for the entire assignment process. Rerun: N GSX Navigator: Y
Create Bellcore ISUP Circuits (*01*96)	Creates one or more ISUP Circuits (CICs) associated with an ISUP Service Group and assigns them to channels on one or more Ports (Spans). This task skips CICs *97 to *00 per Bellcore specifications. This task automatically sets the admin state to enabled and operational state to in service for all circuits created. A full description of the fields on this screen follows: Shelf defaults to 1.

Task Name	Task Description
	Slot the slot associated with the server module whose channels will be associated with CICs. DS3 Index the index associated with the DS3 used in forming the names of the spans using the default circuit span naming convention. If creating circuits on a T1 card, this parameter should be 0. If creating circuits on a T3 card, this parameter should be 1. The default setting is 1. ISUP Service Name the named reference to an existing ISUP Service Group. Circuit Service Profile the named reference to an existing circuit service pro file. This parameter is optional. Span Start the starting span for circuit assignment. This parameter defaults to 1. Span End the ending span for circuit assignment. This parameter can be as high as 28 (for a T1 on a T3) or as high as 12 for a T1. The default setting is 28. Channel Start the channel number to start with in the circuit assignment process for each specified span. This parameter is used in conjunction with the CICs per Port parameter (specified below) to determine the contiguous range of channels to be associated with the CICs. This range will be identical for all Spans. This parameter defaults to 1. CIC Start the CIC number to start with for the entire assignment process. CICs per Port the number of CICs to assign to channels on each Port (Span). The maximum number that should be used is 24. By default this screen creates CICs across all T1 spans within a T3. If you are provisioning a T1 card (cns10/cna10 server/ adapter pair), set the 0 and Num Ports to a maximum value of 12. The number of CICs created and assigned to channels is equal to: Num Ports X CICs per Port The contiguous range of channels used across all specified Ports is equal to: CIC Start to CICs per Port Rerun: N GSX Nav: Y

BT IUP Provisioning

This category of tasks provides for the configuration of BT IUP Services.

Many BT IUP provisioning tasks include the **Stop if element exists** field. When set to **Yes** (the default), this setting stops the task from executing if a GSX object with the specified name already exists. This prevents existing GSX entries (such as inservice Trunk Groups) from being inadvertently overwritten when new objects are provisioned. When set to No, the task executes without checking for previously-defined element names.

Task Name	Task Description
Create BT IUP Trunk Group Profile	Creates a trunk group profile and assigns it to existing carrier code and SS7 Node name references. Also, automatically sets the profiles admin state to enabled. Both the carrier code and the SS7 Node references must exist on the GSX9000 before calling this task. Rerun: Y GSX Nav: Y
Create BT IUP Trunk Group	Creates a trunk group and assigns it a carrier code and SS7 Node reference. This task automatically sets the trunk groups admin state to enabled. Both the carrier code and the SS7 Node references must exist on the GSX9000 before calling this task. Rerun: N GSX Nav: Y
Create BT IUP Trunk Group using Profile	Creates a trunk group with parameters obtained from the references trunk group pro file. This task automatically sets the trunk groups admin state to enabled. The trunk group profile must exist on the GSX9000 before calling this task. Rerun: N GSX Nav: Y
Create BT IUP Service Profile	Creates an BT IUP service profile that references an existing trunk group profile. This task automatically sets the service profiles admin state to enabled. The trunk group profile must exist on the GSX9000 before calling this task. Rerun: N GSX Nav: Y

Task Name	Task Description
Create BT IUP Service	Creates and configures an BT IUP service group with references to a trunk group and service profile. This task automatically sets the service groups admin state to enabled and operational state to in service. The trunk group and service profile (if provided) references must exist on the GSX9000 when this task is called. The service profile name is optional. All other fields are mandatory. SGX Configuration (Create CC Client) For every BT IUP Service with a new DPC, you must create a Call Control Client entry at the SGX. You can accomplish this task automatically by providing the correct values in the following fields. • Automatically Configure SGX: This determines if automatic SGX configuration will be performed or not • Dual CE: Yes, if dual CE is in use, otherwise No • (MNS1) Host Name 1: DNS name for GSX IP address 1 • (MNS1) Alternate Host Name 1: DNS name for GSX IP address 2 • (MNS2) Host Name 2: DNS name for GSX IP address 3 • (MNS2) Alternate Host Name 2: DNS name for GSX IP address 4 • Point Code Format: Format of the Destination Point Code previously entered. Rerun: N GSX Nav: Y

Task Name	Task Description
Create BT IUP Circuits on 8 Span E1	Creates one or more BT IUP Circuits (CIC's) associated with an BT IUP Service Group and assigns them to channels on one or more Spans. This task automatically sets the admin state to enabled and operational state to in service for all circuits created. A full description of the fields on this screen follows: Shelf : defaults to 1. Slot: the slot associated with the server module whose channels will be associated with CICs. BT IUP: Service Name The named reference to an existing BT IUP Service Group. Circuit Service Profile: The named reference to an existing circuit service profile. This parameter is optional. Span Start: The span to begin circuit assignment at. This parameter defaults to 1. Span End: The span to end circuit assignment at. This parameter can be as high as 8. The default setting is 8. Channel Start: The starting channel number in the circuit assignment process for each specified span. The system uses this parameter in conjunction with the CICs per Port parameter (specified below) to determine the contiguous range of channels associated with the CICs. This range is identical for all Spans. This parameter defaults to 1. CIC Start: The starting CIC number for the entire assignment process. CICs per Span: The number of CICs to assign to channels on each Span. The maximum number that should be used is 31. The number of CICs created and assigned to channels is equal to: Num Spans X CICs per Span Rerun: N GSX Nav: Y
Create BT IUP Circuits on 12/36 Span E1	Identical to "Create BT IUP Circuits on an 8 Span" except that this task is tailored to CIC assignment across a 12/36 Span E1. Rerun: N GSX Nav: Y
Create BT IUP Circuits on 84 T1/63 E1 Spans	Identical to "Create BT IUP Circuits on an 8 Span" except that this task is tailored to CIC assignment across up to 84 Span T1 or 63 Span E1. Rerun: N GSX Nav: Y

ISDN Provisioning

This category of tasks support ISDN provisioning for PRI Lines and for NFAS. There is a single special purpose task for PRI. There are 4 separate tasks you must execute in sequence to provision ISDN NFAS.

Many ISDN provisioning tasks include the **Stop if element exists** field. When set to **Yes** (the default), this setting stops the task from executing if a GSX object with the specified name already exists. This prevents existing GSX entries (such as inservice Trunk Groups) from being inadvertently overwritten when new objects are provisioned. When set to **No**, the task executes without checking for previously defined element names.

Task Name	Task Description
Create ISDN Trunk Group Profile	Creates a trunk group profile. This task automatically sets the profiles admin state to enabled. Rerun: Y GSX Nav: Y
Create ISDN Trunk Group	Creates a trunk group and assigns it a carrier code reference. This task automatically sets the trunk groups admin state to enabled. The carrier code reference must exist on the GSX9000 before calling this task. Rerun: N GSX Nav: Y
Create ISDN Trunk Group using Profile	Creates a trunk group with parameters used from the references trunk group pro file. This task automatically sets the trunk groups admin state to enabled. The trunk group profile must exist on the GSX9000 before calling this task. Rerun: N GSX Nav: Y
Create Simulated Facility Group	Creates a Simulated Facility Group. This task automatically sets the group's admin state to enabled. Rerun: N GSX Nav: Y
Create ISDN Service Profile	Creates a service profile. This task automatically sets the profiles admin state to enabled. Rerun: N GSX Nav: Y
Create ISDN Switch Profile	Creates a switch profile. This task automatically sets the profiles admin state to enabled. Rerun: N GSX Nav: Y

Task Name	Task Description
Create ISDN PRI Trunks	Creates and configures one or more ISDN PRI trunks and assigns them to channels ranges on the specified circuit spans. The format of the names for the ISDN Services created for each span are as follows: <Prefix><Shelf>><Slot> for a T1 and E1, <Prefix><Shelf><Slot><DS3Index> for a T1 Span on a T3, where Prefix is the Service Name Prefix field specified in the form. This prefix defaults to "PRI". This task assumes that each specified circuit span will use an ISDN interface of 0. A full description of the fields on this screen is as follows: Service Name Prefix: The textual prefix used in the construction of the ISDN service name. Port Name Prefix: The textual prefix used in identifying the Circuit name on a T3, T1, or E1 per the default circuit naming convention. For circuit spans on a T3 or T1 use "T1". Use "E1" for an E1 span. Trunk Group: Name reference to an existing trunk group. Primary DChannel Timeslot: The channel number to use for the DChannel (default = 24). Shelf defaults to 1. Slot: The slot associated with the server module whose channels will be associated with the ISDN bchannels. DS3 Index: The index associated with the DS3 used in forming the names of the spans using the default naming convention documented Servers. If creating circuits on a T1 or E1 card, set this parameter to 0. If creating circuits on a T3 card, set this parameter to 1 (default = 1). Span Start: The starting span for circuit assignment This parameter defaults to 1. Span End: The ending span for circuit assignment on (inclusive). the maximum value is 12 for a T1, and 28 for a T3. The default setting is 28. BChannel Start: The starting channel number in the circuit assignment process for each specified span. Use this parameter in conjunction with the BChannel End parameter to form a contiguous range of BChannels. This range is identical for the contiguous range of specified spans (default = 1). BChannel End: The ending channel number (default = 23). The system sets each ISDN service, ISDN interface, and set of B Channels state to administratively enabled and in service. Rerun: N GSX Nav: Y

Task Name	Task Description
Create ISDN NFAS Service Group	Creates and configures an ISDN Service used for NFAS. This task should be used in conjunction with the following three tasks in order to create primary and backup ISDN interfaces, additional interfaces (if any), and the BChannel service(s). Rerun: N GSX Nav: Y
Create ISDN Channel Service	Creates and configures an ISDN BCHANNEL Service. Bchannel service can be added to a trunk group. It includes the call processing subset of ISDN configuration parameters. Bchannel are added to a BCHANNEL service by configuring the Bchannels with the BCHANNEL service name. A BCHANNEL service can only be applied to the Bchannels of one DCHANNEL service. Rerun: N GSX Nav: Y
Create ISDN Channel Service	Creates and configures an ISDN DCHANNEL Service. Dchannel service is a service associated with Dchannel and cannot be added to a trunk group. Interfaces are added to this type of service. Also, Bchannel maintenance is done with this service. Rerun: N GSX Nav: Y

Task Name	Task Description
Create ISDN Primary/Backup Interface	Creates and configures a Primary or Backup ISDN interface and assigns the DChannel interface to the specified service group. Service Name: The service group name created in the task above. Port Prefix: The textual prefix used in identifying the Circuit name on a T3, T1, or E1 as per the default circuit naming convention. For circuit spans on a T3 or T1, "T1" should be used. "E1" should be used for an E1 span. Shelf defaults to 1. Slot: the slot associated with the server module whose channel will be associated with the ISDN DChannel based on timeslot. DS3 Index: The index associated with the DS3 used in forming the names of the spans using the default naming convention documented under Servers. If creating circuits on a T1 or E1 card, this parameter should be 0. If creating circuits on a T3 card, this parameter should be 1. The default setting is 1. Span: The circuit span associated with the server module for the DChannel. This can be between 1 and 28 for a T3, between 1 and 12 for a T1, or between 1 and 8 for an E1. The default is 1. Type: Primary or Backup interface. Interface: The Interface identifier. Can be between 0 and 19 or 1 and 20. DChannel Timeslot: The channel on the server module to assign as the primary or backup DChannel timeslot. This task automatically places the DChannel in service. Rerun: N GSX Nav: Y

Task Name	Task Description
Create Additional ISDN Interfaces	Creates and configures additional ISDN interfaces and assigns them to the service name provided. Interface numbers used for primary and/or backup must not be duplicated here. Service Name: The service group name created in the task above. Port Prefix: The textual prefix used in identifying the Circuit name on a T3, T1, or E1 as per the default circuit naming convention. For circuit spans on a T3 or T1, "T1" should be used. "E1" should be used for an E1 span. Shelf defaults to 1. Slot: The slot associated with the server module whose channel will be associated with the ISDN DChannel based on timeslot. DS3 Index: The index associated with the DS3 used in forming the names of the spans using the default naming convention documented under Servers. If creating circuits on a T1 or E1 card, this parameter should be 0. If creating circuits on a T3 card, this parameter should be 1. The default setting is 1. Span Start: The starting circuit span to begin creating additional interfaces. Interface Start: The starting interface number. Num Interfaces: The number of interfaces to create. There is currently support for up to 18 additional interfaces. Rerun: N GSX Nav: Y

Task Name	Task Description
Configure ISDN NFAS BChannel Service	Creates and configures ISDN BChannels of DCHANNEL service and assigns them to the BCHANNEL service name provided. DService Name: The service group name that associated with the Dchannel. BService Name: The service group that can be added to a trunk group. Bchannels are added to a BCHANNEL service group. Interface Start: The starting interface number. The primary and backup interfaces should be included in this range. Num Interfaces: The number of interfaces to configure BChannels for. There is currently support for up to 20 interfaces. Primary Interface: The primary interface number created above. Backup Interface: The backup interface number created above. Primary DChannel Timeslot: The channel on the server module to assign as the primary DChannel timeslot. Backup DChannel Timeslot: The channel on the server module to assign as the backup DChannel timeslot. BChannel Start: The starting Bchannel number assign to the BCHANNEL service. Num Bchannels: The number of Bchannels to configure on each specified interface. Trunk Member Start: The starting Trunk Member number to use when assigning to BChannels. BChannel Direction: The direction of traffic allowed on the designated channels. Circuit Profile: The name of the circuit service profile applying to the designated Bchannels. Operational Mode: The Bchannel's operational mode. After configuration, this task automatically places the DChannel and Bchannel services in service, enabled the interfaces and places the assigned Bchannels in service. Rerun: N GSX Nav: Y

Task Name	Task Description
Configure ISDN BChannels BService of DService	Creates and configures ISDN B-Channels of DCHANNEL service and assigns them to the BCHANNEL service name provided. DService Name: The service group name that associated with the D-channel. BService Name: The service group that can be added to a trunk group. B-channels are added to a BCHANNEL service group. Interface Start: The starting interface number. The primary and backup interfaces should be included in this range. Num Interfaces: The number of interfaces to configure B-Channels for. There is currently support for up to 20 interfaces. Primary Interface: The primary interface number created above. Backup Interface: The backup interface number created above. Primary DChannel Timeslot: The channel on the server module to assign as the primary D-Channel timeslot. Backup DChannel Timeslot: The channel on the server module to assign as the backup D-Channel timeslot. BChannel Start: The starting B-channel number assign to the BCHANNEL service. Num Bchannels: The number of B-channels to configure on each specified interface. Trunk Member Start: The starting Trunk Member number to use when assigning to B-Channels. BChannel Direction: The direction of traffic allowed on the designated channels. Circuit Profile: The name of the circuit service profile applying to the designated B-channels. Operational Mode: The B-channel's operational mode. After configuration, this task automatically places the D-Channel and B-Channel services in service, enabled the interfaces and places the assigned B-channels in service. Rerun: N GSX Nav: Y

Task Name	Task Description
Assign ISDN Channels to BService	Assigns ISDN BCHANNEL(s) to designated BCHANNEL service. Rerun: N GSX Nav: N

CAS Provisioning

This category of tasks supports the creation and configuration of trunk groups, and digit collection profiles used by the CAS objects. This category also provides configuration of CAS collection profiles, CAS signaling sequences and conditions, and CAS service groups, profiles and CAS channels.

Many CAS provisioning tasks include the **Stop if element exists** field. When set to **Yes** (the default), this setting stops the task from executing if a GSX object with the specified name already exists. This prevents existing GSX entries (such as inservice Trunk Groups) from being inadvertently overwritten when new objects are provisioned. When set to No, the task executes without checking for previously defined element names.

Task Name	Task Description
Create CAS Trunk Group Profile	Creates a trunk group profile. This task automatically sets the profiles admin state to enabled. Rerun: N GSXNav: Y The creation using profile is not necessary if the parameter is already in the profile.
Create Trunk Group	Creates a trunk group and assigns it a carrier code reference. This task automatically sets the trunk groups admin state to enabled. The carrier code reference must exist on the GSX9000 before calling this task. Rerun: N GSX Nav: Y
Create CAS Trunk Group using Profile	Creates a trunk group with parameters used from the references trunk group pro file. This task automatically sets the trunk groups admin state to enabled. The trunk group profile must exist on the GSX9000 before calling this task. Rerun: N GSX Nav: Y

Task Name	Task Description
Create CAS Collection Profile	Creates a CAS collection profile. Rerun: N GSX Nav: Y
Create CAS Signaling Sequence (SSP)	Creates a CAS signaling sequence profile and adds a new token to the profile. If the profile already exists the token and its parameters are added to the sequence at the specified position. Rerun: N GSX Nav: Y
Create CAS Signaling Sequence (SSP) Table	Creates one or more entries within a CAS signaling sequence profile. Up to 32 entries are supported. Rerun: N GSX Nav: Y
Create CAS Signaling Condition (SCP)	Creates a CAS signaling condition profile and adds a new token to the profile. If the profile already exists the token and its parameters are added to the sequence at the specified position. Rerun: N GSX Nav: Y
Create CAS Signaling Condition (SCP) Table	Creates one or more entries within a CAS signaling condition profile. Rerun: N GSX Nav: Y
Create CAS Service Group Profile	Creates a CAS service group profile. The administrative state of the profile is automatically enabled after configuration. Rerun: N GSX Nav: Y
Create CAS Service Group	Creates a CAS service group. The system sets the administrative state of the service group to enabled after configuration. Rerun: N GSX Nav: Y
CAS Service Group using Profile	Similar to Create CAS service group except that a profile is used rather than specified parameters. The system set the administrative state of the service group to enabled after configuration. Rerun: N GSX Nav: Y

Task Name	Task Description
Create CAS Channel(s) on T3	Same as Create CAS Channel(s) except that the Span Start and End values default to 1 and 28 respectively. Rerun: N GSX Nav: Y
Create CAS Channel(s) on 12/36 Spans T1/E1	Same as Create CAS Channel(s) except that the Span Start and End values default to 1 and 12/36 respectively. Rerun: N GSX Nav: Y
Create CAS Channel(s) on 3xT3	Same as Create CAS Channel(s) except that the port start and end and span start and end values are tailored to a CNS60/CNS80/CNS85 card. Rerun: N GSX Nav: N
Create CAS Channel(s) on 84 T1/63 E1 Spans	Same as Create CAS Channel(s) except that the span start and end values are tailored to a CNS71/CNS82/CNS86 card. Rerun: N GSX Nav: N
Create CAS Channel(s)	Creates one or more CAS Channels associated with an CAS Service Group and assigns them to channels on one or more Spans. This task automatically sets the admin state to enabled and operational state to in service for all channels created. Configure the T1 port for Robbed Bit signaling prior to referencing it. A full description of the fields on this screen follows: Shelf (GSX9000 only) defaults to 1. Slot (GSX9000 only) : The slot associated with the server module which these channels will reference. DS3 Index (GSX9000 only): The index associated with the DS3 used in forming the names of the spans using the default circuit span naming convention. If creating circuits on a T1 card (CNS10/CNA10 server/adaptor pair), set this parameter to 0. If creating circuits on a T3 card, set this parameter to 1. The default setting is 1. CAS Service Name: The named reference to an existing CAS Service Group. Circuit Profile Name: The named reference to an existing circuit service pro file. This parameter is optional.

Task Name	Task Description
	Span Start: (GSX9000 only) The starting span to begin channel assignment. This parameter defaults to 1. Span End: (GSX9000 only) The ending span for channel assignment. This parameter can be as high as 28 (for a T1 on a T3) or as high as 12 for a T1. The default setting is 28. Port Start: The starting port to begin channel assignment. If creating circuits on a T1 card (CNS10/CNA10 server/adapter pair), set this parameter to 1. Port End: The ending port for channel assignment. This parameter can be as high as 24. If creating circuits on a T1 card (CNS10/CNA10 server/adapter pair), set this parameter to 1. Channel Start: The starting channel number in the channel assignment process for each specified span or port. This parameter defaults to 1. Channel End: The ending channel number in the channel assignment process for each specified span or port. This range will be identical for all spans or ports. This parameter defaults to 1. Trunk Member Start: The starting trunk member value to be used during the entire configuration process. This parameter is empty by default. Rerun: N GSX Nav: Y

IP Provisioning

Creates and configures IP Trunk Groups used by SIP, H323, and Gateway Service Groups.

Task Name	Task Description
Create IP Network Selector Table	Creates an IP Network Selector Table for use with an IP Trunk Group. Rerun: N GSX Nav: N
Create Linked IP Trunk Group	Create a Linked IP Trunk Group. Rerun: N GSX Nav: N
Create Selected IP Trunk Group	Create a Selected IP Trunk Group. Rerun: N GSX Nav: N

Task Name	Task Description
Create SIP Service Group	Create a SIP Service Group. Rerun: N GSX Nav: N A new parameter, NO_ATTEMPT_CDR_URI USERNAME is added. This parameter specifies the name of the URI for which ATTEMPT CDR should not be generated when a SIP INVITE has been received with the specified value in request URI and/or From header.
Configure SIP Service Group	Configures a SIP Service Group. Two new parameters are added. • SRTIMER STATE Specifies the support of Suspend Resume timer (SR Timer). The SR Timer will be started when sip INFO suspend (SUS) message is received for the configured SIP-I service group. When resume (RES) INFO message is not received within the specified SR timer, the GSX sends BYE to both the endpoints and terminates the call gracefully. But if resume message is received within expiry of SR timer, the GSX cancels the timer and continue the call. • SRTIMER VALUE SET The Suspend Resume timer (SR Timer) in seconds. The default value is 30 seconds
Create H323 Service Group	Create an H323 Service Group. Rerun: N GSX Nav: N
Create Gateway Service Group	Create a Gateway Service Group. Rerun: N GSX Nav: N
Create IPSec Policy	Creates a named IP Security policy, which associate an IKE Peer database and a Security Policy database. Rerun: N GSX Nav: Y
Create IPSec IKE Peer Database	Creates an Internet Key Exchange Peer database, which is a list of SIP peers that are eligible for protected sessions using IPsec, and associates it with a IP Security Policy. Rerun: N GSX Nav: Y

Task Name	Task Description
Create IPSec Security Policy Database	Creates a Security Policy database, which is an ordered list of rules that specify the type of protection to provide for each packet that subjected to the rule, and associates it with a IP Security Policy. Rerun: N GSX Nav: Y

GR303 Provisioning

Creates and configures GR303 Interface Groups.

Task Name	Task Description
Create Interface Group	Create and configure a GR303 Interface Group. Rerun: Y GSX Nav: N
Add port	Adds and configures a GR303 Interface Group's Port. Rerun: Y GSX Nav: N
Add CRV	Add and configure a CRV to a GR303 Interface Group. Specify a single value, such as 10, or specify a the range of values, such as 1030. Rerun: Y GSX Nav: N

Diameter Provisioning

Implements the Diameter AAA (Authentication, Authorization, and Accounting) base protocol as specified in RFC 3588 on the GSX/SBC 9000 platform.

Task Name	Task Description
Create Diameter Node	Creates the new diameter node object. Rerun: Y GSX Nav: Y
Create Diameter Route	Creates and configures a new diameter route for hosting the realm route table. Rerun: Y GSX Nav: Y
Create Diameter Peer	Creates and configures the diameter peer hosting all the peer connections. Rerun: Y GSX Nav: Y

Miscellaneous

Task Name	Task Description
Create PSTN Static Call	Creates and configures the two endpoints involved in a PSTN static call. All fields are mandatory. Rerun: Y GSX Nav: N
Create Packet Static Call	Creates and configures the two endpoints involved in a Packet static call. All fields are mandatory. Rerun: Y GSX Nav: N
DiffServ Create IP Filter	Creates and configures an IP filter used for differentiated services. All fields are mandatory. Rerun: Y GSX Nav: N
DiffServ Mark IP Filter	Marks the differentiated services code point for an existing IP filter. All fields are mandatory. Rerun: Y GSX Nav: N
Create IP Input Filter	Creates and configures IP Input Filter. IP Input Filter and Protocol fields are mandatory. This task automatically sets the IP Input filter admin state to enabled. Rerun: Y GSX Nav: N
Configure Packet to Packet State	Sets the administrative state of packet to packet routing capabilities in this GSX. Rerun: Y GSX Nav: Y
Configure Logical Signaling Address Binding State	Sets the state of logical signaling address binding as either: disabled In this state, the GSX does not respond to ARP requests for logical addresses. These logical addresses must be reachable on all NIFs and the NEXT HOP router/switch must have proper static routes to direct traffic to these addresses. enabled (default) In this state, the GSX will respond to ARP requests for logical addresses. This condition allows you to configure logical signaling addresses on the same subnet as other NIFs. The benefits of this state are described above. Rerun: Y GSXNav: Y

Task Name	Task Description
Configure Script Cache Size	Configure Script Cache Size for Level 1 and 2. Rerun: Y GSX Nav: N
Configure Announcement	Configures Announcement. All fields are mandatory. Rerun: Y GSX Nav: N
Create Announcement Package	Creates an Announcement Package. Rerun: Y GSX Nav: Y
Add Announcement to Announcement Package	Adds an Announcement to the designated Announcement Package. Rerun: Y GSX Nav: N
Create Local Name Service	Creates and configures Local Name Service with user defined record name and the hostname used for lookup. The hostname must be unique across all records. Rerun: N GSX Nav: Y
Create PathCheck Ping Path	Creates the path on which the recurring ping requests and replies are issued. Rerun: Y GSX Nav: Y
Create IP ACL	Creates IP Access Control List Filters. Rerun: Y GSX Nav: N
Create ISDN DChannel Monitor	Creates a passive monitor of both the receive and transmit side of the Dchannel, as two separate clear channel calls. Rerun: N GSX Nav: Y

Task Name	Task Description
CAS Test Call Initial Setup	Configures CAS Test Call Initial Setup, which is the initial setup used to create the CAS Signaling Sequence Profiles (SSPs) and the Collection profile required for configuring a CAS service to perform test calls. The following SSPs are created: outTestCic: Performs the outgoing test call on a specific CIC. Called party number is preconfigured. outTestDs0: Performs the outgoing test call on a specific DS0 (slot/port/channel). Called party number is preconfigured. outTestCicCdDtmf: Performs the outgoing test call on a specific CIC. Called party number is entered through DTMF. outTestDs0CdDtmf: Performs the outgoing test call on a specific DS0 (slot/port/channel). Called party number is entered through DTMF. inTest: Performs the incoming test call. Called party number is preconfigured. inTestCdDtmf: Performs the incoming test call. Called party number is entered through DTMF. psxTest: Performs PSX Configuration Test. The following Collection Profile is created: testCdNum The profiles listed above should not exist prior to running this task. If they do, they should be deleted first. Rerun: N GSX Nav: Y
CAS SSP Update for OutGoing Test Call	This task provides an easy method to update a CAS SSP for outgoing test calls. Rerun: Y GSX Nav: Y
CAS SSP Update for Incoming Test Call	This task provides an easy method to update a CAS SSP for incoming test calls. Rerun: Y GSX Nav: Y
CAS Service Update SSP	Updates a CAS Service SSP. Rerun: Y GSX Nav: Y

Task Name	Task Description
Configure IP ACL State	Defines the IP ACL state. Rerun: Y GSX Nav: Y

Mtrm Provisioning

Creates and configures commands for Master Trunk Group.

Task Name	Task Description
Create Client MTRM Connection	Creates and configures a client MTRM connection. Rerun: Y GSX Nav: N
Create Server MTRM Connection	Creates and configures a server MTRM connection. Rerun: Y GSX Nav: N
Create Master Trunk Group Server	Creates and configures a Master Trunk Group server. Rerun: Y GSX Nav: N
Create Master Trunk Group Client	Creates and configures a Master Trunk Group client. Rerun: Y GSX Nav: N
Configure Master Trunk Group Connection Reset	Configures a Master Trunk Group connection reset. Rerun: Y GSX Nav: N

GSX Upgrade Automation

In this section:

- [Overview](#)
 - [GSX Upgrade Automation Overview](#)
 - [GSX Automated Upgrade Process Overview](#)
 - [Prerequisites](#)
- [Importing GSX Software Packages for NFS Based GSX Upgrade](#)
- [Importing GSX Software Packages for Local Disk Based GSX Upgrade](#)
- [View GSX Software Packages Imported to RAMP](#)
- [View GSX Software Report](#)
- [Initiate an Upgrade](#)
- [Create an Audit Log Report](#)
- [Copy GSX Configuration to an FTP Server](#)

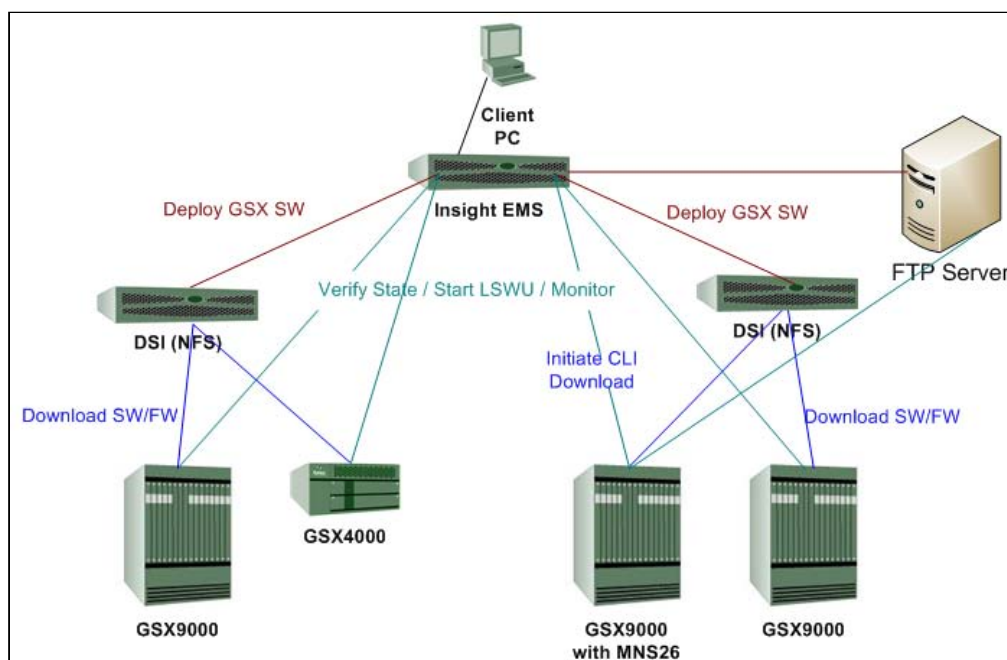
Overview

You can import GSX release packages to Ribbon Application Management Platform (RAMP) and upgrade GSX9000 devices in your network using the packages. The upgrade process is performed on a Job/Task basis, where each job can contain multiple GSX upgrade tasks.

You can run up to four tasks simultaneously from a Job and 16 tasks (default) across RAMP. Refer to [GSX Upgrade Parameters](#).

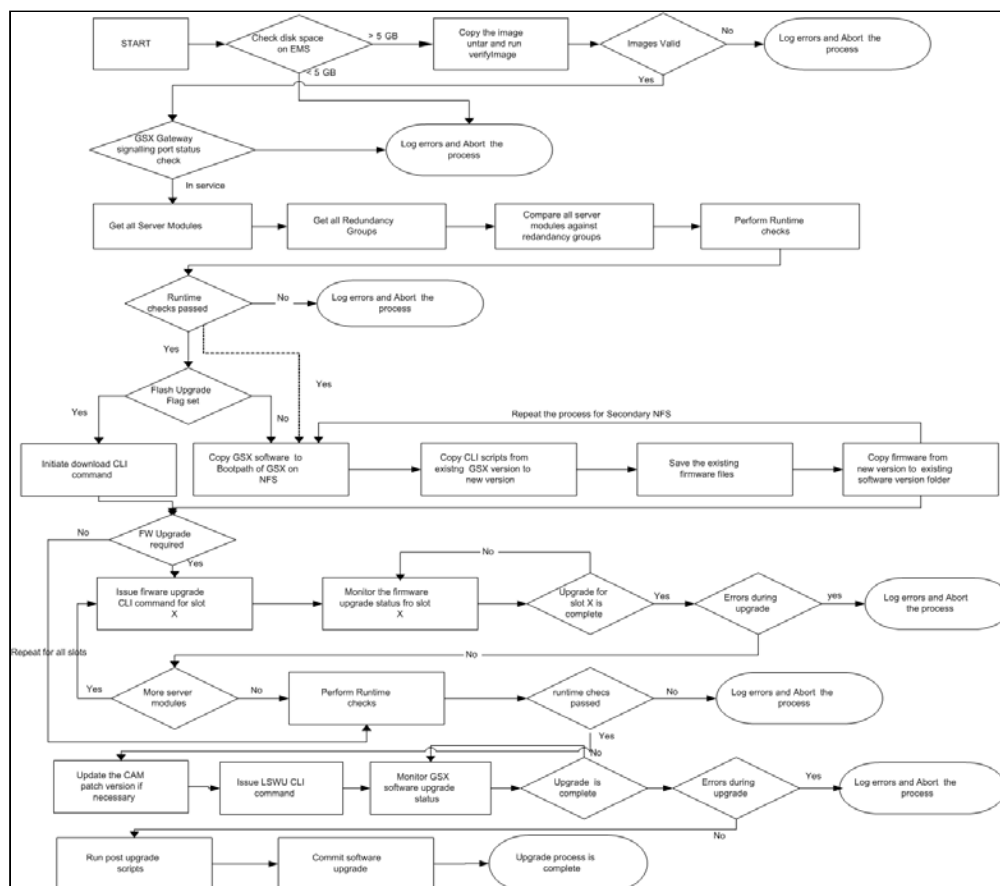
Refer to the [GSX Release Notes](#) for the software releases that support the upgrade.

GSX Upgrade Automation Overview



The following figure provides a more detailed view of the process operations.

GSX Automated Upgrade Process Overview



- **GSX SW (Software) Packages** allow you to:
 - Import and validate GSX software packages.
 - Access GSX software reports, which displays version and status of registered GSX devices.
- **Upgrade Jobs** allow you to:
 - Create, launch, and monitor GSX Upgrade jobs.
 - Access audit logs and GSX software reports.

Note

Never use multiple **RAMP devices** to manage the same DSI/NFS server while performing GSX upgrades. Attempting to do so may result in incomplete upgrades that could impact GSX call processing and performance.

Note

From DSI v15.1 onwards, the "root" user is disabled by default. Enable the "root" user manually under `/etc/ssh/sshd_config` file, restart the service, discover the DSI with "root" credentials in the node registration page and then initiate the GSX upgrade.

Prerequisites

- Possess Super User [privileges](#) for **Configuration Management** under **Core Resources**.
- Possess Devices [privileges](#) under **Device Management**.

Importing GSX Software Packages for NFS Based GSX Upgrade

Start

In order to make a software package available for upgrade, import it to RAMP. You must have access to the package (tar file) to import.

1. Log on to the RAMP GUI.
2. Navigate to **Operations > GSX Upgrade Automation > SW Packages**.
3. Click **Import**.
4. Perform one of the following depending on the location of the package:
 - a. If the package is stored on RAMP, select the radio button **EMS server** and enter the path in **Release Package Path**.
 - b. If the package is stored on a client PC, select the radio button **Client PC** and choose the file.
 - c. If the package is stored on an **SFTP/FTP** server, select the radio button **SFTP/FTP Server** and details of the SFTP/FTP server: **IP Address**, **User Name**, **Password**, **Confirm Password**, and **Package Location**. After designating the path, click the **OK** button to start importing.

Importing GSX Software Packages for Local Disk Based GSX Upgrade

Start

For Local Disk upgrade, the Software package can be imported using the following options:

1. **RAMP Server**: If the package is stored on RAMP, select the radio button, the EMS server and enter the path in Release Package Path.
2. **Client PC**: If the package is stored on a client PC, select the radio button **Client PC** and choose the file.
3. **SFTP/FTP Server**: If the package is stored on an SFTP/FTP server, select the radio button **SFTP/FTP Server** and details of the SFTP/FTP server. For SFTP import, ensure SFTP is enabled on the GSX.

The SFTP/FTP server option enables GSX to download GSX SW image directly from the RAMP server to its local disk over SFTP, using the GSX automated install command during the upgrade phase. Enable the SFTP on GSX to proceed with the upgrade. The File transfer mode on the GSX has to be **SFTP**. If SFTP is not enabled, the upgrade gets aborted with an error message.

The above options are used to download the SW image to the following locations on RAMP:

1. `/opt/sonus/ems/weblogic/sonusEms/data/gsxSwStaging` - For RAMP to explore the SW package and display contents in GUI.
2. `/home/guauser/gsxSw/` - This path is used for SFTP import. It enables GSX to download SW image to its local disk over SFTP. A dedicated SFTP user 'guauser' is used for the GSX upgrade.
3. For FTP import, the GSX downloads the SW image from the specified FTP server to its local disk.

The Local Disk upgrade screen has the following information.

- **GSX Name** - the name of the GSX node.

- **GSX Version** - the GSX software version.
- **Boot Path** - the current setting on the GSX.
- **File Transfer** - the mode on the GSX.
- **State** - the current status of the upgrade.

View GSX Software Packages Imported to RAMP

Start

1. Log on to the RAMP GUI.
2. Navigate to **Operations > GSX Upgrade Automation > SW Packages**. The valid and invalid software packages imported to RAMP display. RAMP lists valid packages by the version number. These packages are available for use by upgrade jobs. RAMP may list invalid packages by version number or by the name of the imported tar file, depending upon the reason they failed validation during the import operation. The following details display for every software package:
 - **Version**—the software version.
 - **File Name**—the name of the tar file.
 - **File Size**—the size of the tar file in bytes.
 - **Time of the last modification**—the timestamp for the last modification of the file.
 - **GSX9000 Max CAM Patch Version**—the highest version of the CAM patch available for the GSX9000 in this software package.
 - **Card Type**—(GSX9000) the card type for the associated firmware.
 - **Firmware Name**—the firmware image name for the associated card type.
 - **Firmware Version**—the firmware version for the associated card type.

View GSX Software Report

The GSX Software Report options displays software version information for all registered GSX nodes. If the nodes have been included in an Upgrade Job, RAMP populates additional fields concerning the Job. You can sort the table based upon any column by clicking the column name.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Node Management > GSX Upgrade Automation > SW Packages**.
3. Click **GSX SW Report**. Clicking the name again sorts the column in the opposite direction.
 - **GSX Name**—the name of the GSX node.
 - **Current Version**—the version of software currently running on the GSX node.
 - **Target Version**—if the node is included in a Job, this is the software version targeted by the upgrade.
 - **Job Name**—the name of the Job that includes the upgrade task for this GSX node.
 - **Upgrade Status**—the current status of the upgrade Job for this node.

Controls in the upper right corner of the report allow you to print the current report, refresh the information displayed, or close the report. The report also has export controls (beneath the table) that allows export of the report information in csv or XML format.

Initiate an Upgrade

The **Upgrade Jobs** window is divided into two frames (panes). The left pane displays an object tree representing the current status of Upgrade Jobs. The possible statuses are:

- **Created**—category for new, unexecuted Upgrade Jobs. You can only modify Jobs in the created category.
- **In Progress**—category for Jobs/Tasks currently executing.

- **Completed**—category for Jobs/Tasks that ran successfully.
- **In Error**—category for Jobs/Tasks automatically stopped due to an encountered error requiring manual resolution.
- **Aborted**—category for Jobs/Tasks manually aborted.

When a job contains multiple upgrade tasks, if any of the tasks are in progress, the job defaults to the In Progress state. This applies even if other tasks include a combination of created, completed, in error or aborted states.

Expanding any tree object and clicking on a Job results in the display of configuration and state information in the right pane. This interface also has two groups of control buttons.

In the upper right corner, there are three buttons. You can use the **Delete** button to delete any unlocked Job in either the Created, Aborted, or Completed categories. You can use the **Modify** button to change the settings for any unlocked Job in the Created category. The **Lock/Unlock** button allows the creator of the Job or anyone with Insight Administration Super User privileges, to lock the Job preventing any configuration changes or deletions. Locking a Job also disables the Associated Task buttons discussed below.

The Upgrade Task area contains five control buttons and a table displaying the details of each GSX upgrade task within the Job. The table supplies the following information for each GSX: GSX Name, Original GSX Version, State (of the upgrade process), and Start/Finish Time.

If the GSX Name field includes a Magnifying Glass icon, you can click the icon for additional information.

Ensure all GSX nodes included in the upgrade job are currently registered. The created task must not include any purged nodes.

After you select one or more GSXs by checking the check box and depending upon its State, you can use the Upgrade Task buttons to execute particular operations. The buttons and functions are:

- **Start**—starts the upgrade task for the selected GSX(s). The Job moves to the In Progress category.

If you did not supply the root user password for the DSI system on the node registration page, Insight will request the password after you click the Start button.

DSI 'root' is disabled by default from DSI 15.0 onwards. Hence enable the 'root' on DSI before you proceed with upgrading the GSX.

- **Abort**—aborts the upgrade task for the selected GSX(s). The Job moves to the Aborted category. You can only abort a task, if the jobs are in any of these states "UPGRADE_TASK_CREATED", "ERROR", "ABORTED", "COMMIT_REQUIRED", "SW_UPGRADE_READY", "FW_VERSION_MISMATCH"
- **Upgrade FW**—initiates a firmware upgrade task on the selected GSX(s).
- **Upgrade SW**—initiates a software upgrade task on the selected GSX(s).
- **Commit**—commits the new / SOFTWARE path to nonvolatile memory.

Upgrade Task State Definitions

States	Definition
UPGRADE_TASK_START	Upgrade Task initiated
SW_COPIED_PRI_NFS	Indicates that the software release package is copying to the primary DSI/NFS.
SCRIPTS_COPIED_PRI_NFS	Indicates that the Scripts are copying to the primary DSI/NFS.
SW_COPIED_SEC_NFS	Indicates that the software release package is copying to the secondary DSI/NFS.
SCRIPTS_COPIED_SEC_NFS	Indicates that the Scripts are copying to the secondary DSI/NFS.
GSX_UPGRADE_READY	Indicates readiness to proceed with the GSX upgrade process.
RUNTIME_CHECK_VERIFIED	The required runtime checks are performed on the target GSX. These checks include: • verify the Gateway to Gateway Signaling Port is Inservice • verify the GSX is in fully protected mode • verify the Link State statistics
FW_VERSION_MISMATCH	Indicates that the firmware currently running on one or more GSX cards is older than the firmware in the upgrade package, but the Automatic Firmware Upgrade was not selected. The user must initiate the firmware upgrade or proceed without upgrading the firmware.
FW_UPGRADE_RUNNING	The firmware upgrade is in process.
SW_UPGRADE_READY	The software upgrade portion of the operation is ready to run.
SW_UPGRADE_RUNNING	The software upgrade is in process. For a fully populated GSX9000 the software upgrade could require between 2 and 3 hours.
SW_UPGRADE_FINISHED	The software upgrade portion of the operation has completed.
COMMIT_REQUIRED	Indicates that the software upgrade completed successfully and the GSX is in commit required state. User action is required to permanently commit the software version. If not committed, the GSX reverts to its previous software version upon reboot.
POST_UPGRADE_SCRIPT_RUNNING	Indicates that a post-upgrade script is running.

States	Definition
GSX_UPGRADE_FINISHED	The upgrade task has completed successfully.
ABORTED	Indicates that the upgrade task was aborted.
ERROR	Indicates that the upgrade task is in an error state.
FTP_GSX_SW_STARTED	Indicates that the GSX upgrade task is started.
FTP_GSX_SW_FINISHED	Indicates that the GSX upgrade download task is completed.

1. Log on to the RAMP GUI.
2. Navigate to **Operations > GSX Upgrade Automation > Upgrade Jobs**.
3. Click **New Job**.
4. In **Upgrade to Version**, select the version of GSX to which you want to upgrade.
5. In **Job Name**, enter a name for this upgrade job. Ensure the name is unique only contains alphanumeric characters.
6. Select the GSXs you want to include in this upgrade job by highlighting them in the **Available GSXs** list and moving them to the **GSXs to Upgrade** list using the right arrow button. The list of available GSXs includes all GSXs accessible by the user and not already associated with other jobs.
Ensure that all GSXs in a job are running the same (major.minor.point) version of software. For example, RAMP will not allow a job to contain a GSX using V13.02.03 and another GSX using V13.02.04. Build version differences are allowed. For example, two GSXs running V13.02.04R002 and V13.02.04R003 respectively can be in the same job.
7. Select **Copy Scripts** if you want the script files copied from the current software release directory in the GSX system tree to new software release directories on the DSI/NFS. The default value is unchecked.

If you select the **Copy Scripts** option, when starting an upgrade job, the system does the following as part of the software copy operations:

copies the sysinit.tcl and sessinit.tcl files in cli/sys from the old version to the target version
copies all files under cli/scripts/* from the old version to the new version.

8. If the GSX software contains multiple CAM patch versions, in **Target CAM Patch Version**, select the CAM patch version to which you wish to upgrade. This selection applies to all GSXs in the job.

The default value for the **CAM Patch Version** is "0" if the upgrade is to a software version where the minor and/or major version numbers are different (for example, 713.02.04 to 15.01.00). The default **CAM Patch Version** will be the same as the version currently configured on the GSX, if the major and minor versions are the same (for example, 13.02.03 to 13.02.04). The default value is **NONE** if the new GSX version does not support CAM patch version.

9. In the **Firmware Upgrade** section select the following options:
 - **Enforce Firmware Upgrade** — determines whether the system forces a firmware upgrade prior to the software upgrade, assuming new firmware is available. If you do not select the **Automatically Upgrade the Firmware** option, the upgrade job halts until you initiate the firmware upgrade using the **Upgrade FW** button. The default value is checked.

- **Automatically Upgrade the Firmware** (enabled when **Enforce Firmware Upgrade** is selected) — determines whether the system attempts to automatically upgrade the firmware on each GSX included in this job. The default value is checked.
10. In the **Select Post-upgrade Script** section, if you want to automatically run a script after the completion of the upgrade, select **Run Post-upgrade Script** and enter the path to the script in the designated field. If you select **Stop On Error**, the post-upgrade script stops if it encounters an error. If you leave the box unchecked (default) the script continues to run to completion even if it encounters errors executing some commands.
 11. Click **OK** to save the job.

Create an Audit Log Report

RAMP logs the progress/issues for each GSX Upgrade/Copy Job as it proceeds. You can access the log files, define filter criteria, and create reports containing information concerning each subtask associated with one or more upgrade jobs.

RAMP can generate audit log files from devices that are configured with IPv4 or IPv6 address type.

Start

To create an audit log report, perform the following procedure:

1. Log on to the RAMP GUI.
2. Navigate to **Operations > GSX Upgrade Automation > Upgrade Jobs**.
3. Click **Audit Log**.
4. Select a **From** and **To** date/time range for the report by clicking the appropriate button and selecting/setting the date and time. The To field defaults to the current date/time, while the From field defaults to 3 months earlier.
5. Enter filter information into one or more of the following fields **Job(s)**, **GSX(s)**, **User(s)**, or **Description**. You can set multiple entries in each field by using a comma for separation. The definitions of the fields are:
 - a. **Job(s)**—The name of the job.
 - b. **GSX(s)**—The node name of the GSX on which the action/activity was performed. You must use the complete node name.
 - c. **User(s)**—The name of the user initiating the job. You must use the complete user name.
 - d. **Description**—Any text or portion of text that appears in the Description field related to an action/activity.

Filter criteria of different types are ANDed, while multiple entries of a particular criteria type are ORed. For example, entering Test123 in the Job field and Boston1, Boston2, and Boston3 in the GSX field would result in the generation of a report that included any information for the GSXs: Boston1, or Boston2, or Boston3 only if that information concerned Job: Test123.

All fields are case sensitive. Wildcards are allowed in all fields except the Description.

6. Click **View** to run the report and display the results.

The top portion of the report displays the settings used to create the report, including the date you created the report along with the filter information. The example shown had filters for a particular date range and for the Job: test.

The bottom portion of the display is the body of the report. Insight shows each subtask associated with an Upgrade Job is on an individual line initially sorted based upon the Date (timestamp) field. The other fields in the

report are: Job Name, GSX Name, Use Name, and (Task) Description. You can sort the table based upon any column by clicking the column name. Clicking the name again sorts the column in the opposite direction.

Additionally, controls in the upper right corner of the interface allow you to print the current report, or close the report interface. The interface also has export controls that allows export of the report information in either csv, Excel, or XML format.

Copy GSX Configuration to an FTP Server

You can create a job to copy GSX configuration to an FTP server.

The possible statuses on the RAMP GUI after you initiate copying (copy job) the configuration:

- **Created**—category for new, unexecuted Upgrade Jobs. You can only modify Jobs in the created category.
- **In Progress**—category for Jobs/Tasks currently executing.
- **Completed**—category for Jobs/Tasks that ran successfully.
- **In Error**—category for Jobs/Tasks automatically stopped due to an encountered error requiring manual resolution.
- **Aborted**—category for Jobs/Tasks manually aborted.

Note

When a job contains multiple copy tasks, if any of the tasks are in progress, the job defaults to the In Progress state. This is the case even if **other tasks include** a combination of created, completed, in error or aborted states.

Expanding any tree object and clicking on a Job results in the display of configuration and state information in the right pane. This interface also has two groups of control buttons.

In the upper right corner, there are three buttons. You can use the Delete button to delete any unlocked Job in either the Created, Aborted, or Completed categories. You can use the Modify button to change the settings for any unlocked Job in the Created category. The Lock/Unlock button allows the creator of the Job or anyone with Insight Administration Super User privileges, to lock the Job preventing any configuration changes or deletions. Locking a Job also disables the Associated Task buttons discussed below.

The Copy Task area contains two control buttons and a table displaying the details of each GSX upgrade task within the Job. The table supplies the following information for each GSX: GSX Name, Original GSX version, State (of the upgrade process), and Start/Finish Time.

Note

If the GSX Name field includes a Magnifying Glass icon, you can click the icon for additional information.

After you select one or more GSXs by checking the checkbox and depending upon its State, you can use the File Copy Job Tasks buttons to execute particular operations. The buttons and functions are:

- **Start**—starts the copy task for the selected GSX(s). The Job moves to the In Progress category. Once the job is started the user is prompted for FTP Server Passwords input.
- **Abort**—aborts the copy task for the selected GSX(s). The Job moves to the Aborted category.
- **Copy Announcement**—initiates a copy announcement task on the selected GSX(s).
- **Copy Tcl Script**—initiates a copy Tcl script task on the selected GSX(s).

Copy Task State Definitions

States	Definition
DOWNLOAD_TASK_CREATED	Indicates the Download Job is created.
DOWNLOAD_TASK_STARTED	Indicates the Download Job is started.
GSX_VERSION_NOT_FOUND_ERROR	Indicates the current GSX Version is not present in GSX Software Version list.
FTP_LOCAL_DISK_SYNCING	Indicates that the SYNC process is going on between active and passive MNS cards.
COPYING_ANNOUNCEMENT_FILE_IN_PROGRESS	Indicates that the Copying of Announcement files job is in progress.
COPYING_TCL_SCRIPTS_IN_PROGRESS	Indicates that the Copying of Tcl Scripts job is in progress.
COPYING_TCL_SCRIPTS_COMPLETE	Indicates that the Copying of Tcl Scripts is completed.
COPYING_ANNOUNCEMENT_FILE_COMPLETE	Indicates that the Copying of Announcements file is completed.
DOWNLOAD_TASK_FINISHED	Indicates the Download Job is completed successfully.
COPYING_TCL_SCRIPTS_ERROR	Indicates that the Copying of Tcl Scripts job is failed.
COPYING_ANNOUNCEMENT_FILE_ERROR	Indicates that the Copying of Announcements file job is failed.

To create new FTP Files Copy Job:

Start

1. Log on to the RAMP GUI.
2. Navigate to **Operations > GSX Upgrade Automation > Copy Jobs**.
3. Click **Copy Jobs**.
4. In the **Select GSXs** section, enter the name for the Copy Job in **Job Name**. Ensure the name is unique and contains only alphanumeric characters.
5. Select the GSXs you want to include in this Copy Job by highlighting them in the **Available GSXs** list and moving them to the **GSXs to Upgrade** list using the right arrow button. The list of available GSXs includes all GSXs accessible by the user with MNS26 cards.
6. In the **Enter FTP Server Details** section, enter the following details:
 - **IP Address**—The IP address of the FTP server.
 - **User Name**—The username to use to access the FTP server.
7. In the **Enter FTP Job Details** section, enter at least one of the following details:
 - **Announcement Files**—The path for the announcement files.
 - **TCL Scripts**—The path for the TCL scripts.
8. Click **OK** to save the Job.

Authentication and Authorization

In this section:

- [Authentication Methods RAMP Supports](#)
 - [Local Authentication](#)
 - [LDAP Authentication](#)
 - [SAML Authentication](#)
 - [RADIUS Authentication](#)
- [RAMP's Authorization Model](#)
 - [Roles](#)
 - [Resource Groups](#)
 - [User Groups](#)
 - [Users](#)
- [Multi-Tenancy Support \(Optional\)](#)
 - [Tenant Configuration](#)
 - [Tenant User Authentication](#)

Related articles:

- [Authentication and Authorization Workflows](#)
- [Configure Multi-Tenancy](#)
- [Add Users](#)
- [Add User Groups](#)
- [Configure Authentication Methods](#)
- [Locations](#)
- [Manage Certificates](#)
- [Monitor User Activity](#)
- [Terminate User Sessions](#)
- [Set Session Expiry in RAMP GUI](#)
- [Authentication and Authorization Administration](#)
- [EdgeView Service Administration](#)

The Ribbon Application Management Platform (RAMP) Authentication and Authorization (A/A) service determines who can access the RAMP GUI/API/CLI and what operations users are permitted to do. The A/A service supports multiple ways to authenticate users and a wide range of controls to manage user privileges and access to resources. Each deployment must determine which options are the best fit with their security and business objectives. The following sections provide an overview of the A/A service and the features it supports.

Authentication Methods RAMP Supports

The RAMP A/A service supports four mechanisms for authenticating users:

- Local authentication against the local RAMP database.
- Lightweight Directory Access Protocol (LDAP) authentication against an external Directory Server.
- Security Assertion Markup Language (SAML) v2.0 authentication against an external identity provider (IdP).
- Remote Authentication Dial-In User Service (RADIUS) authentication to support Password Authentication Protocol (PAP).

The default mechanism is local authentication against credentials stored in the RAMP database. However, the A/A service supports authentication against external, third-party systems like directory server or an IdP, in addition to local authentication. The A/A service allows an administrator to specify in which order to apply authentication methods if more than one is configured.

Local Authentication

RAMP's local authentication configuration is managed as the local security realm. In this model, RAMP administrators add users to the system and the A/A service locally stores user information, including usernames and passwords. Users log in through the RAMP-provided login window and their credentials are checked against the data in the local security realm.

RAMP administrators configure password complexity rules and user ID/password aging rules for the local security realm and RAMP enforces these for users who use local authentication.

Within the local authentication model, RAMP provides a default “admin” user account with an initial password of “admin.” The “admin” user has full privileges to perform RAMP operations. An administrator must log in as the “admin” user in order to begin setting up the system for the first time. For security, first steps should include setting a new, secure password for the admin user account. Refer to [Change User Password](#) for the procedure to change a user password. Logged in as admin, an administrator can also configure one of the external security realms as the primary method of user authentication.

However, even if one of the alternative realms is configured, Ribbon strongly recommends that all RAMP deployments maintain the configuration of the local security realm to support the default admin user seeded in the local database. This ensures that there is a way to access the system if there is a problem with the external security realm.

For information on configuring the local security realm, refer to [Configure Local Authentication](#).

LDAP Authentication

The A/A service supports LDAP authentication. In this model, information on individual users is stored in an external LDAP-compatible Directory Server such as a Microsoft Active Directory service. Users log in through the RAMP-provided login window, but their credentials are forwarded to Directory Server using LDAP for authentication. In a successful authentication response, the LDAP server returns a RAMP user group name that determines what sort of user privileges to grant the user.

On RAMP, an administrator must configure an LDAP security realm that specifies how to access the LDAP server (address and credentials) and how to retrieve and interpret data from the LDAP database, including the attribute that contains the RAMP user group name. An administrator must also create user groups that correspond to the user groups identified in the LDAP responses.

Note

LDAP authentication is qualified with the third party LDAP servers OpenLDAP and Microsoft Active Directory (AD) as qualified third-party LDAP servers.

For information on configuring an LDAP security realm, refer to [Configure LDAP Authentication](#).

SAML Authentication

The A/A service also supports SAML-based authentication by an external IdP. This model often supports single sign-on scenarios. For SAML-based authentication, users do not log in using the RAMP login window. Instead, from a web browser, users begin by logging into their IdP login window. The IdP is responsible for authenticating the user and may require steps such as multi-factor authentication. After the IdP authenticates the user, the user selects the RAMP application from the options provided by the IdP. The IdP submits a signed SAML assertion to the RAMP A/A service for the user. When the A/A service successfully validates the signature, RAMP’s main application page opens.

In the SAML assertion, the IdP must also return a RAMP user group name that determines what sort of user privileges to grant the user.

On RAMP, an administrator must add an X.509 certificate that validates the signature the IdP provides. The A/A service provides an interface for uploading trusted certificates. The administrator must also configure a SAML security realm that points to the IdP certificate and that identifies the returning attribute that contains the RAMP user group name. If the user opts to encrypt their SAML assertions, the realm must also point to the

certificate to use to decrypt the assertion. An administrator must also create user groups that correspond to the user groups identified in the SAML assertions.

Note

SAML authentication is qualified with the third party tool OKTA Idp.

For information on configuring a SAML security realm, refer to [Configure SAML Authentication](#).

RADIUS Authentication

The A/A service also supports RADIUS-based authentication. In this model the authentication is done externally on the RADIUS server. When users log in to RAMP, the user name and password are collected and sent to the RADIUS server for authentication. This authentication is provided using PAP (Password Authentication Protocol). RAMP uses Vendor Specific Attribute (VSA) to associate and authenticate user groups configured on RAMP and the RADIUS realm. The RADIUS realm supports IPv4 and IPv6 addresses without any difference in the configuration and functioning.

RAMP connects to the RADIUS realm over User Datagram Protocol (UDP) using the RADIUS server's hostname and port configured in the RADIUS realm. If RAMP receives an Access-Accept message from the RADIUS server, then the user is authorized to access the RADIUS realm.

On RAMP, an administrator must configure a RADIUS security realm that specifies how to access the RADIUS server and how to retrieve and interpret data from the attribute that contains the RAMP user group name. An administrator must also update the configuration files user name, password, and user groups in the `users` file and the host name, RAMP IP address, and shared secret in the `clients.conf` file on the RADIUS server.

Note

The compatibility between the RADIUS authentication server and the RAMP is validated with the third-party RADIUS servers, FreeRADIUS and Cisco ISE.

For information on configuring a RADIUS security realm, refer to [Configure RADIUS Authentication](#).

RAMP's Authorization Model

The A/A service employs a role-based model for authorizing user access to specific features and services within RAMP. For the purpose of assigning privileges, the resources within RAMP are grouped into five application areas:

- Authentication and Authorization
- Core Resources
- Device Management
- Fault Management
- License Management
- PSX Management
- Performance Management
- SBC Provisioning Role for API and CLI

Each application area controls access to one or more actions or resources. Four key configuration objects allow an administrator to manage users and roles.

Roles

Roles define sets of privileges for performing actions or accessing resources. Depending on the type of resource or action, the privilege levels available can differ. For many resources, users are either granted permission to them or they are not. However, some resources support multiple privilege levels (Operator, Provisioner, Super User) to enable aligning privileges with different job responsibilities. For example, the Performance Management application supports an Operator privilege level for users whose access should be limited to work with performance reports.

For more information on the specific resources within each application area and the privilege levels they support, refer to [User Privileges in RAMP](#).

For more information on creating user roles, refer to [Set Privileges for Users by Adding Roles](#).

Resource Groups

Resource groups define sets of managed devices to enable a deployment to apply policies to a group of devices collectively. Although resource groups are defined within Device Management, they are an essential component of authorization policy on **RAMP**.

For information on creating resource groups, refer to [Create Resource Groups](#).

User Groups

User groups combine a selected role with a selected resource group. Members of the user group have the privileges defined by the role for the devices defined by the resource group. Through user group assignments, administrator determine not only the level of access to an application, such as fault management, but also to which devices within the network the privilege extends.

For more information on creating user groups, refer to [Add User Groups](#).

Users

Users added on **RAMP** are part of the local security realm. **RAMP** locally stores their login credentials and they are subject to the policies set for the local security realm such as password complexity rules and password aging rules. The **RAMP** administrator assigns privileges to local users by adding them to the user group(s) that include the appropriate privileges for the appropriate set of devices. Note that users that authenticate using one of the external realms (LDAP or SAML or RADIUS) do not have user accounts stored on **RAMP**. **RAMP** determines which user privileges to extend to external users by the user group returned as an attribute during the authentication process.

For more information on creating users, refer to [Add Users](#).

Multi-Tenancy Support (Optional)

RAMP supports multi-tenancy to enable separating the users and resources of a large network into distinct tenant environments. Businesses with multiple sub-organizations can use tenants to further control access and policies for different groups.

To implement multi-tenancy, **RAMP** provides a “tenant” parameter on four of the key A/A configuration objects: users, user groups, roles, and security realms that when configured make the objects tenant-specific. However, multi-tenancy is an optional deployment model. By default **RAMP** assigns the top-level (root) tenant to any new A/A objects. Thus **RAMP** is a single tenant environment unless an administrator adds tenant-level configuration as described in the following sections.

Tenant Configuration

The process to create distinct tenant environments requires both defining specific tenants and effectively managing tenant-specific A/A objects. The process begins with a top-level RAMP administrator defining a new tenant. RAMP provides the tenant-administration privilege to the default “admin” account that is in the root tenant. To ensure that proper tenant restrictions are in place, top-level (root tenant) administrators must manage all tenant-level administration.

For more information on creating tenants, refer to [Configure Multi-Tenancy](#).

Tenants

By default RAMP adds new tenants directly below the top-level, root tenant. However, RAMP allows multiple levels within a tenant hierarchy so that an administrator can also create a tenant that is a sub-tenant of another tenant. Within tenant configuration, the tenant that contains another tenant is called its “parent” tenant.

Roles

A role can be mapped to a tenant. The RAMP administrator must add tenant-specific roles that enable users to perform necessary tasks, but restricts user access to actions or resources that potentially cross the boundaries of the tenant.

User Groups

The RAMP administrator must ensure that a tenant-specific user group associates with the proper group of tenant-specific users.

Security Realms

Currently, RAMP supports multi-tenancy for deployments using the local security realm for authentication. There is a single local realm for the RAMP system and users are associated with their specific tenant in their user configuration.

Tenant User Authentication

Tenant users must authenticate with RAMP using a tenant-specific URL. This URL incorporates an external tenant ID that RAMP assigns to the tenant when the administrators adds the tenant. Thus the RAMP administrator must share this specific URL with the appropriate tenant users. The format of the URL is: `https://<RAMP address>?tenantId=<external tenant ID>`

For more information on logging in as a tenant user, refer to [Configure Multi-Tenancy](#).

Authentication and Authorization Workflows

The following workflows outline the main steps required to complete key Authentication and Authorization tasks on Ribbon Application Management Platform (RAMP). Each step links to a page where you can obtain detailed information and procedures.

- [User Group and Privilege Management](#) – configure user privileges to access resources.
- [User Management](#) – configure user authentication parameters.

Workflow – User Group and Privilege Management

Step	Action
1	Create user roles to define sets of privileges for performing actions or accessing resources.

Step	Action
2	Create resource groups to define sets of managed devices..
3	Create user groups to link resource groups and roles.

Workflow – User Management

Step	Action
1	Configure security realms to determine how users authenticate.
2	Create local users and add them to the user groups.

Configure Multi-Tenancy

Use the following procedure to define a tenant. After you define the tenant you can select it when you configure users, roles, and user groups as needed. Refer to the "Multi-Tenancy Support" section on [Authentication and Authorization](#) for more information on multi-tenancy.

By default RAMP assigns the top-level (root) tenant to any new objects added within the A/A service. Thus RAMP is a single tenant environment unless an administrator adds tenant-level configuration.

Prerequisites

Tenant Administration privileges within **Authentication and Authorization**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Tenants**.
3. Click **Add Tenant**. The **Tenant Details** pane displays.
4. Enter a name for the tenant in the **Tenant Name** field.
5. Select a parent from the **Parent Tenant Name** list.
6. Enter a description for the tenant.
7. Click **Save**.
8. Add a role for the tenant. Refer to [Set Privileges for Users by Adding Roles](#).
9. Add a user group for the tenant. Refer to [Add User Groups](#)
10. Add a user under the tenant group. Refer to [Add Users](#).
11. To log on to the RAMP GUI as a tenant:
 - a. Navigate to **Management > Authentication & Authorization > Tenants**.
 - b. Find the External Tenant ID for the tenant you want to log in.
 - c. Append the RAMP URL with the External Tenant ID in the following format: https://<RAMP IP address or FQDN>/?tenantId=<External Tenant ID for the tenant>. Example: https://10.11.12.13/?tenantId=0215c0a7-bf70-435a-af9a-c5c9d25f72b9
 - d. In the RAMP login window, enter the username and password for the tenant user.

Add Users

Related articles:

- [Set Privileges for Users by Adding Roles](#)
- [Manage Users](#)

Add users on Ribbon Application Management Platform (RAMP) to be part of the local security realm. The RAMP A/A service manages users added to the local security realm. If you use an external authentication method, user records are stored in those external systems, they are not managed by the RAMP A/A service.

RAMP automatically creates a default user account "admin" with full privileges to RAMP resources for use in setting up and maintaining your system. Refer to [Authentication and Authorization](#) for more information.

Prerequisites

User and Role Administration [privileges](#) in **Authentication and Authorization**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Users**. The **Users** window displays.
3. Click **Add User**. The **Add User** window displays.
4. If you are implementing multi-tenancy, select the [tenant](#) for the user from the **Tenant** list. The user is assigned to the root tenant by default.
5. The user is enabled by default. To disable the user, toggle the "User" button.
6. To force the user to change password upon initial login, enable **Force Password Change**.
7. To force the user to change the password after a set period time, enable **Password Aging**. For more information on password aging, refer to [Configure Local Authentication](#).
8. To add the user to user groups, from the **User Groups** pane, select a user group under the **Available** column and add it under **Selected** column.
9. To set localization parameters for the RAMP GUI, in **Custom Properties** select a region and default country.
10. Click **Save**.

Set Privileges for Users by Adding Roles

In this section:

- [Create a Duplicate Role](#)
- [Edit a Role](#)
- [Delete Roles](#)

Related articles:

- [User Privileges in RAMP](#)

A role is a collection of privileges that defines the level of access users have to different service and features (resources) within Ribbon Application Management Platform (RAMP).

The levels available depend on the resource. Refer to [User Privileges in RAMP](#) for privileges associated with every resource.

A role "admin" is created by default. A user group "admin" is mapped to the admin role.

Prerequisites

You must have **User and Role Administration** [privileges](#) in **Authentication and Authorization**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Roles**. The **Roles** window displays.
3. Click **Add Role**. The **Add Role** pane displays.
4. Enter a name for the role.
5. If you are implementing multi-tenancy, select the [tenant](#) for the role from the **Tenant** list. The role is assigned to the root tenant by default.
6. Enter a description of the role.
7. Click **Save**.
8. Click **Actions** against every application listed.
9. Select a privilege type or enable privileges for each resource shown. For more information on permissions within applications, refer to [User Privileges in RAMP](#).
10. Click **Save**.
11. Click **Close**.

Create a Duplicate Role

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Roles**. The **Roles** window displays.
3. Click on the name of the role that you wish to duplicate. The **Role Details** pane displays.
4. Click **Create Duplicate Role**. The **Role Details** pane displays.
5. Enter a name for the role.
6. Click **Save Duplicate Role**.

Edit a Role

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Roles**. The **Roles** window displays.
3. Click on role name. The **Role Details** pane displays.
4. Modify role details.
5. Click **Save**.

Delete Roles

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Roles**. The **Roles** window displays.
3. Perform one of the following:
 - To delete a role:
 - i. Click the delete button under "Actions" against a role name. A dialog box displays to confirm.
 - ii. Click Yes.
 - To delete multiple roles at once:
 - i. Select multiple roles.
 - ii. From the "Bulk Action" menu, select "Delete."
 - iii. Click Yes to confirm.

User Privileges in RAMP

In this section:

- [Resources with Multiple Privilege Levels](#)
- [Resources with Enable or Disable Permissions](#)

- [PSX Specific Permissions](#)
- [SBC Specific Permissions](#)

The permissions available in the Ribbon Application Management Platform (RAMP) are listed in this section.

Resources with Multiple Privilege Levels

Each resource with multiple privilege levels includes an option "None." Set the privilege to "None" to restrict a user from accessing a resource category within RAMP. You can set different privilege levels to a user for RAMP resources based on user tasks.

Application	Resource	Privileges
Core Resources	API	Access to API
	CLI	Read Commands
		Write Commands
		Scripts
	Configuration Management	Read-Only Commands
		Read-Write Commands
		SuperUser Commands
	GUI	Access to GUI
	Health Reports	View
		Execute
		Schedule
	Insight Administration	Administrator
	Tools	Network Diagnostics
Fault Management	Fault Management	Alarm Monitoring
		Alarm View Management

		Advanced Fault Management
Performance Management	Performance Management	Performance Reports
		Data Collection and Threshold Configuration

Resources with Enable or Disable Permissions

You can enable or disable access to the following resource based on user tasks.

Application	Privileges	Privilege Details
Authentication and Authorization	- User and Role Administration - Realm Administration - Certificate Administration - Tenant Administration	
Device Management	- Devices - Devices > Administration - Devices > Resource Groups - Inventory Reports - Job Status - Scheduled Jobs - Firmware Repositories - Auto Provisioning - Provisioning Status - Provisioning Policy - EdgeMarc Profiles	When the Devices option is disabled, then Administration and Resource Groups are disabled automatically. When the Devices option is enabled again, the Administration and Resource Groups option needs to be manually enabled. For admin role, the Devices, the Administration and the Resource Groups options are enabled by default.
License Management	License Management Administration	Permission to view and modify configurations under License Management Administration
	Reports Operations	Permission to perform all reports operations under Manual Reports and Post-Paid Reports
	License Operations	Permission to perform all license management operations such as license installation, license revocation, and license association.

Application	Privileges	Privilege Details
	View Licenses and Reports	Read-only permission to view feature licenses, license profiles, and reports.

PSX Specific Permissions

You can set read and write permissions for PSX entities based on user tasks.

Application	Privileges
PSX Management	Read and write permission for each of the PSX entities

SBC Specific Permissions

Application	Privileges	Privilege Details
SBC API/CLI Access Role	None	No access to any space.
	Administrator	- Permission to read common commands & data spaces - Permission to write common commands & data spaces - Permission to access sensitive administrative functions - Permission to manage security & audit functions - Permission to view security & audit logs
	FieldService	- Permission to read common commands & data spaces - Permission to write common commands & data spaces
	Guest	Permission to read common commands & data spaces
	Operator	- Permission to read common commands & data spaces - Permission to write common commands & data spaces
	SecurityAuditor	Permission to view security & audit logs.

Manage Users

In this section:

- [Edit Local Users](#)
- [Disable Local Users](#)
- [Delete Local Users](#)

To see a list of RAMP users, navigate to **MANAGEMENT > Authentication & Authorization > Users**. The **Users** window contains:

- A list of local users (stored in the RAMP database) appears on the **Provisioned Users** tab. You can edit, disable, and delete local users, except the admin user.
- A list of external users currently logged into RAMP using access tokens appears on the **External Users** tab. External users are authenticated through an external realm and have access tokens that authorizes them to use RAMP resources.

The count of tokens listed for each user indicates the number of active sessions associated with that user.

Edit Local Users

You can edit local users.

Prerequisites

User and Role Administration [privileges](#) in **Authentication and Authorization**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Users**. The **Users** window displays.
3. Click the **Provisioned Users** tab.
4. Click on the username.
5. Modify user details.
6. Click **Save**.

Disable Local Users

You can disable local users.

Prerequisites

User and Role Administration privileges in **Authentication and Authorization**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Users**. The **Users** window displays.
3. Click the **Provisioned Users** tab.
4. Perform one of the following:
 - To disable a user:
 - i. Toggle the "User Status" button against a user.
 - ii. Click Yes to confirm.
 - To disable multiple users:
 - i. Select the multiple users.
 - ii. From the "Bulk Action" menu, select "Disable."
 - iii. Click Yes to confirm.

Delete Local Users

You can delete local users.

Prerequisites

User and Role Administration privileges in **Authentication and Authorization**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Users**. The **Users** window displays.
3. To delete a user:
4. Click the **Provisioned Users** tab.
5. Perform one of the following:
 - To delete a user:
 - i. Click the delete button under "Actions" against a user.
 - ii. Click Yes to confirm.
 - To delete multiple users:
 - i. Select the multiple users.
 - ii. From the "Bulk Action" menu, select "Delete."
 - iii. Click Yes to confirm.

Add User Groups

In this section:

- [Edit a User Group](#)
- [Delete User Groups](#)

Use the following procedure to create a user group in Ribbon Application Management Platform (RAMP). A user group combines user privileges (roles) with devices (resource groups). Users assigned to the same user group share the same privileges to the same devices. A user can be added to multiple user groups.

Prerequisite

User and Role Administration [privileges](#) in **Authentication and Authorization**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > User Groups**. The **User Groups** window displays.
3. Click **Add User Group**. The **Add User Group** window displays.
4. Enter a name and description for the user group.
5. If you are implementing multi-tenancy, select the [tenant](#) for the user group from the **Tenant** list. The user group is assigned to the root tenant by default.
6. From the **Users** pane, select the users you want to include in the user group from the **Available** column and add them under the **Selected** column.
7. Perform the following in the **Resource Groups** pane:
 - a. Select resource groups that you want to allow users to access from the **Available** column and add them under the **Selected** column.

- b. Select a role that provides the privilege level you want users to have for the selected resource group from the **Role** column for the resource group.
8. Click **Save**.

Edit a User Group

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > User Groups**. The **User Groups** window displays.
3. Click on a group name. The Group Details pane displays.
4. Modify group details.
5. Click **Save**.

Delete User Groups

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > User Groups**. The **User Groups** window displays.
3. Perform one of the following:
 - To delete a user group:
 - i. Click **Delete** under "Actions" against a group name.
 - ii. Click **Yes** to confirm.
 - To delete multiple user groups:
 - i. Select multiple user groups.
 - ii. From the **Bulk Action** menu, select **Delete**.
 - iii. Click **Yes** to confirm.

Configure Authentication Methods

In this section:

- [Configure Local Authentication](#)
- [Configure LDAP Authentication](#)
 - [Disable Endpoint Notification for LDAP Over SSL/TLS Connections](#)
 - [Renewing LDAP Certificates](#)
 - [Upload SSL Certificates for LDAP Authentication Over SSL](#)
- [Configure SAML Authentication](#)
 - [Configure Identity Provider](#)
- [Configure RADIUS Authentication](#)
 - [RADIUS Administration](#)
 - [Configure VSA](#)
- [Set Order of Priority for Authentication Methods](#)
- [Enable or Disable Security Realms](#)

Ribbon Application Management Platform (RAMP) supports the following authentication methods:

- Local authentication against a local database
- Lightweight Directory Access Protocol (LDAP) authentication against an external Directory Server

- Security Assertion Markup Language (SAML) v2.0 authentication against an external Identity Provider (IdP)
- Remote Authentication Dial-In User Service (RADIUS) authentication using Password Authentication Protocol (PAP).

Configure Local Authentication

The Ribbon Application Management Platform (RAMP) ships with a default authentication mechanism of local authentication against the local database. A default "admin" user with full administrator privileges is provided with the default password "admin".

To begin using the system, log onto the RAMP GUI as the admin user and immediately change the password for the admin account to a secure value. As the admin user you have access to the full system including configuring local authentication parameters.

A security realm for the local database is created by default with security options you can customize:

Perform the following actions to secure local authentication:

- apply password complexity rules
- enable aging for username and password

Although RAMP supports external authentication methods, Ribbon recommends you maintain the local security realm for the default "admin" user to be able to access RAMP if the external authentication methods fail.

Prerequisites

- Realm Administration [privileges](#) within Authentication and Authorization.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Security Realms**. The **Security Realms** window displays.
3. Click on the local realm. The "local" pane displays.
4. In the **Database Realm Properties** pane in the "User Password Complexity Rules" section, set the complexity rules for user passwords. All options are enabled by default.

Field	Description
No password same as Username	The username and password must be different.
Password should not contain whitespace	The password must not contain space characters.
Minimum password length	The minimum number of characters allowed in the password. Range: 3 to 32 Default: 8.
Maximum password length	The maximum number of characters allowed in the password. Range: 3 to 64 Default: 32

Field	Description
Password contains	The password must meet the following criteria: ◦ At least one upper-case alpha character ◦ At least one lower-case alpha character ◦ At least one numeric character ◦ At least one special character ◦ No two characters repeated consecutively Special characters preferably include any characters on a standard keyboard, however, at a minimum, the shifted numeric key characters: ! @ # \$ % ^ & * ().
Password not reusable time period	The password must not be reused for the set duration. The value should be less than the Password Purge Before value. For more information, refer Authentication and Authorization Administration.

5. In the **Database Realm Properties** pane in the "UserId and Password Aging" section, set aging rules for usernames and passwords. All options are disabled by default.

Field	Description
User ID Aging Threshold	A user ID expires if it is never used within the set duration. NOTE: UserId Aging does not apply to the RAMP default admin user. Supported values: ◦ Minimum: 1 day ◦ Maximum: 3650 days (10 years) ◦ Default: 60 days
Password Aging Threshold	The password expires after the set duration. You can set a new password when you log in after the password expiry. The value should be less than the Password Purge Before value. For more information, refer Authentication and Authorization Administration.
Password Expiration Warning	The setting for how many days in advance you want to be notified of the password expiry. The value should be less than the Password Aging Threshold value. NOTE: It is available to configure only if the Password Aging Threshold is enabled.

6. Click **Save**.
- The users authenticated with the local database are listed in the RAMP GUI: **MANAGEMENT > Authentication & Authorization > Users > Provisioned Users**. The count of tokens listed for each user indicates the number active sessions associated with that user.

Configure LDAP Authentication

Related topics:

- [Disable Endpoint Notification for LDAP Over SSL/TLS Connections](#)
- [Renewing LDAP Certificates](#)
- [Upload SSL Certificates for LDAP Authentication Over SSL](#)

The Ribbon Application Management Platform (RAMP) supports Lightweight Directory Access Protocol (LDAP) for external authentication.

When LDAP authentication is enabled, users are authenticated by the directory server and its response must also include an attribute that specifies which RAMP user group to apply to the user.

To configure LDAP authentication over SSL, upload LDAP SSL certificates to RAMP before configuring authentication. To upload SSL certificates, refer to [Upload SSL Certificates for LDAP Authentication Over SSL](#).

Ensure that local authentication is configured as an alternative method to access RAMP if LDAP authentication fails. Refer to [Configure Local Authentication](#) for configuring local authentication.

Prerequisites

- Realm Administration [privileges](#) in **Authentication and Authorization**.
- A user group is created in RAMP.

Start

1. Log on to the RAMP GUI.
2. Add a security realm for LDAP:
 - a. Navigate to **MANAGEMENT > Authentication & Authorization > Security Realms**.
 - b. Click **Add Security Realm**.
 - c. Enter a name for the realm in the "Security Realm Name" field.
 - d. From the **Type** list, select "LDAP". The **LDAP Realm Details** pane displays.
 - e. If you are implementing multi-tenancy, from the Tenant list, select a tenant.
 - f. Use the following table to enter parameter values in the **LDAP Realm Properties** pane.

Parameter	Description	Example of Microsoft AD	Example for OpenLDAP
LDAP server URL	The fully qualified domain name (FQDN) or the IP address of the directory server. <code>ldap://<IP address of directory server>:<port number></code> or <code>ldap://<FQDN of directory server>:<port number></code> The default LDAP port is 389 (Example: <code>ldap://<IP address or FQDN of directory server>: 389</code>). For LDAPS the default port is 636 (Example: <code>ldaps://<IP address or FQDN of directory server>: 636</code>). If the user authentication queries are specifically targeted for the global catalog, use port 3268 if you were using the port 389. LDAP requests sent to port 3268 are used to search for objects in the entire data hierarchy. Similarly, if the user authentication queries are specifically targeted for the global catalog, use port 3269 if you were using the port 636.	<code>ldap://</code> <code>10.54.84.162:389</code>	<code>ldap://</code> <code>10.34.22.52:389</code>

Parameter	Description	Example of Microsoft AD	Example for OpenLDAP
System Username	The system username of the admin user. The directory server's Administrator Bind distinguished name (DN). The Administrator Bind DN is the domain user who searches the LDAP directory. The Administrator Bind DN, along with the password, enables access to the directory server. This bind operation at the realm level is used to authenticate the client (RAMP application) to the directory server to establish an authorization identity that will be used for subsequent operations (individual user search/authentication request) processed on that connection. RAMP does not allow anonymous connections to the LDAP server. Hence, these fields are mandatory.	rbbnedge\administrator	cn=admin,dc=rbbn,dc=com
System Password	The Administrator Bind DN password. The password along with the configured Administrator Bind DN configured enables access to the directory server. Note: Ribbon recommends setting the domain administrator password to never expire. If the password expires, the system does not communicate with the LDAP server, and all user authentications fail.	Change!@#	Ribbon#123

Parameter	Description	Example of Microsoft AD	Example for OpenLDAP
User DN Template	The template for data structure mapping, as defined within the directory server. RAMP uses User Dn Template based authentication. Example for a typical user DN Template value: cn={0},ou=users,dc=rbbn,dc=com. To compute the bind DN of the client, swap the place holder {0} with the login ID provided by the client. For example, if the login ID provided by the client is "guest", the computed bind DN passed to the Directory Server is cn=guest,ou=users,dc=rbbn,dc=com. Note: This procedure does not work if the users belong to different branches of the LDAP directory information tree. For example, if there are some users under ou=users,dc=rbbn,dc=com and other users under ou=external,dc=rbbn,dc=com, the user Dn Template does not work for all the users.	rbbnedge\{0}	cn={0},ou=users,dc=rbbn,dc=com

Parameter	Description	Example of Microsoft AD	Example for OpenLDAP
Search Base	The location in the directory server where the search for a particular directory object begins. It is also referred as Base DN and it is the starting point where an LDAP searches for users' authentication within your directory. It tells where to look for the requested information. It is denoted as the Distinguished Name (DN) of the search base directory object. For example, dc=rbbn,DC=com.	DC=rbbnedge,DC=com	dc=rbbn,dc=com
Search Filter	A basic LDAP query for searching users based on the mapping of a username to a particular LDAP attribute. This configuration is used to search for the users based on the username in the directory server. The following examples represent commonly used search filters. Examples: (&(objectClass=person)(objectClass=user) (&(objectClass=user)(cn=*Sales*)) Check with your LDAP administrator to specify a search filter that uses the attributes specific to your LDAP environment.	(&(objectClass=user) (objectCategory=Person) (sAMAccountName={0}))	(&(objectClass=groupOfUniqueNames) (uniqueMember=cn={0},ou=users,dc=rbbn,dc=com))

Parameter	Description	Example of Microsoft AD	Example for OpenLDAP
Referral	Indicates how to handle directory server (LDAP) referrals. An LDAP referral provides a reference to an alternate location in which an LDAP request is processed. The Directory System Agent (DSA) can return to the Directory User Agent (DUA) an "LDAP Referral" response for any LDAP request that requires a response (The LDAP Result Code response of "10" and an appropriate set of LDAP URLs. The default value is "ignore"). The options to set Referral are: • ignore • follow Note: If you set Referral to "ignore", the LDAP service provider automatically sends this control along with the request. When searching for a directory, in addition to a few continuation references that show where to obtain further results, the server might generate several search results too. If you set Referral to "follow", the LDAP service provider processes all the normal entries first before following the continuation references.	<code>ignore</code>	<code>ignore</code>

Parameter	Description	Example of Microsoft AD	Example for OpenLDAP
Ignore Partial Result Exception	The parameter for the directory server to ignore partial results. Certain directory server setups can contain unreachable referrals and the resulting PartialResultException must be ignored instead of treating it as an error. Currently, RAMP does not handle these referrals manually in the form of ReferralException. Either the user receives the exception (and the user's results are lost) or all referrals are ignored (if the server is unable to handle them correctly. No solution exists to receive the notification if PartialResultException is ignored (other than in the log). The default value is "true".	true	true
Returning Attribute	The attribute that returns the usergroup for RAMP. If the returning attribute is set as "cn", the LDAP searches in the directory server and retrieves the value stored against the key "cn" for example. The value returned must match the name of the usergroup defined in RAMP. If the user belongs to multiple user groups, the "cn" returns multiple group names. RAMP validates whether the returned usergroup is available in the local database and determines the role of the user.	memberOf If the Returning Attribute is set as "memberOf", the API searches in LDAP and retrieves the value stored against the key "memberOf".	cn If the Returning Attribute is set as "cn", the API searches in LDAP and retrieves the value stored against the key "cn".

- g. Test the connection between the [RAMP](#) and directory server by clicking **Test Connection**.
 - h. Click **Save**. The new security realm is disabled by default.
3. Enable the LDAP security realm to use it. Refer [Enable or Disable Security Realms](#).

4. To set LDAP as the primary authentication method on RAMP, refer to [Set Order of Priority for Authentication Methods](#). The users authenticated with external authentication methods including LDAP are listed in the RAMP GUI, **MANAGEMENT > Authentication & Authorization > Users > External Users**. The count of token listed against each user indicates the number active user sessions.

Disable Endpoint Notification for LDAP Over SSL/TLS Connections

The Ribbon Application Management Platform (RAMP) allows you to disable endpoint notifications for Lightweight Directory Access Protocol (LDAP).

The latest versions of Java (1.8 and above) enable endpoint identification for LDAP over the Secure Socket Layer (SSL) and Transport Security Layer (TLS) by default. This is to improve the robustness of LDAPS (secure LDAP over TLS). This is specific to LDAPS and not for connections over HTTPS. Ensure that your SSL certificates are configured to match the hostnames of your LDAP servers.

The setting `com.sun.jndi.ldap.object.disableEndpointIdentification=true` is a system property used to disable endpoint identification for LDAP over the SSL and TLS connections. Endpoint identification is a security feature that verifies the server's hostname against the hostname in the server's SSL certificate. This is the only option if we do not generate certificates with hostname present either in the Common Name (CN) or Subject Alternative Name.

Note

This procedure is used in certain circumstances where the hostname verification causes issues (such as when the SSL certificate does not match the hostname), but use it cautiously.

Start

1. Set the server environment:
 - a. SSH to RAMP as an `admin` user.
 - b. Change to the `root` user:

```
sudo su -
```

- c. Edit the file `/opt/sonus/auth/apache-tomee/bin/setenv.sh`.
 - d. Uncomment the following line:

```
JAVA_OPTS="$JAVA_OPTS
-Dcom.sun.jndi.ldap.object.disableEndpointIdentification=true
-Djavax.net.ssl.trustStoreType=BCFKS -Djavax.net.ssl.trustStore=/opt/sonus/
auth/config/secure/auth-ms.truststore
-Djavax.net.ssl.trustStorePassword=authms"
```

- e. Save the file.
2. Stop the RAMP. For more information, refer to [How to Start and Stop RAMP](#).
3. Start the RAMP. For more information, refer to [How to Start and Stop RAMP](#).
4. For RAMP GR, repeat step 1 on the standby device and restart both the RAMP active and standby devices. To configure LDAP authentication, refer to [Configure LDAP Authentication](#).

Renewing LDAP Certificates

To ensure uninterrupted Lightweight Directory Access Protocol (LDAP) service, it is essential to periodically renew the LDAP certificate within the Ribbon Application Management Platform (RAMP) before the certificate expires. RAMP monitors the certificates stored in the auth keystore, and if the certificate is on the verge of expiry, RAMP raises the [ribbonCertificateExpiryStatusNotification](#) alarm. If the certificate has already expired, then the [ribbonCertificateExpiredNotification](#) alarm is raised. This renewal is necessary whenever the LDAP certificate expires or is deleted. After updating or removing certificates from the AUTH keystore, a RAMP restart is mandatory to apply the changes and maintain seamless LDAP functionality.

Prerequisites

- **Realm Administration** and **Certificate Administration** [privileges](#) under **Authentication & Authorization**.
- The SSL certificate is retrieved from the directory server.

Renew LDAP Certificates

To renew a certificate, delete the existing one and then upload the new one using the same alias.

Perform the following procedure to renew the LDAP certificates:

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > Authentication & Authorization > Certificates**.
3. From the list of certificates, select the certificate you want to delete. You are allowed to select multiple certificates.
4. From the **Actions** column, click the delete icon to delete the certificate.
5. Click **Yes** to confirm deleting the certificate.
6. Upload LDAP SSL certificate to the RAMP:
 - a. Click **Add Certificate**. The **Add Certificate** window displays.
 - b. Enter the **Alias Name**. If the alias name contains uppercase characters, it is automatically converted to lower-case.
 - c. Browse the certificates and upload.
 - d. Click **Save**. The certificate is listed among the certificates.
7. Restart the RAMP. For more information, refer to [How to Start and Stop RAMP](#).

Upload SSL Certificates for LDAP Authentication Over SSL

The Ribbon Application Management Platform (RAMP) supports Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL) for external authentication. To configure LDAP authentication over SSL, upload LDAP SSL certificates before configuring authentication.

Prerequisites

- **Realm Administration** and **Certificate Administration** [privileges](#) under **Authentication & Authorization**.
- The SSL certificate is retrieved from the directory server.

Perform the following procedure to upload the SSL certificates:

Start

1. Log on to the RAMP GUI.
2. Upload LDAP SSL certificate to RAMP:

- a. Navigate to **MANAGEMENT > Authentication & Authorization > Certificates**.
 - b. Click **Add Certificate**. The **Add Certificate** window displays.
 - c. Enter the **Alias Name**. If the alias name contains uppercase characters, it is automatically converted to lower-case.
 - d. Browse the certificates and upload.
 - e. Click **Save**. The certificate is listed among the certificates.
3. (Optional) Disable the endpoint notifications for LDAPs in the RAMP Authentication and Authorization. For more information, refer to [Disable Endpoint Notification for LDAP Over SSL/TLS Connections](#).

Configure SAML Authentication

In this section:

- [Generate Service Provider Certificate](#)

The Ribbon Application Management Platform (RAMP) supports SAML-based external centralized authentication. RAMP supports SAML 2.0 for third-party Identity Providers (IdP) to provide single sign-on (SSO) for RAMP. An IdP issues SAML assertions about an authenticated subject for cross-domain single sign-on.

For example, if a user group name on RAMP is "userGroupName" then the IdP must return the same value in the attribute group.

Authenticated SAML users do not log into RAMP using the RAMP login window. Instead, users log into their IdP and use a shortcut to access RAMP. If the user is authenticated successfully, the RAMP Dashboard displays. If authentication fails, the user is redirected to the RAMP login page.

RAMP supports only signed SAML assertions. An X.509 certificate is used for validating the signature of SAML assertion the IdP provides. If you configure SAML to be encrypted, upload a RAMP certificate for the IdP to encrypt SAML assertions.

Note

Ensure that local authentication is configured as an alternative method to access RAMP if SAML authentication fails. For more information, refer to [Configure Local Authentication](#).

Prerequisites

- A user group is created in RAMP.
- **Realm Administration** and **Certificate Administration** [privileges](#) under **Authentication and Authorization**.
- The URL "https://<RAMP IP address>/coreGui/ui/logon/sso.jsp" is added as the RAMP service provider in your IdP.

Start

1. Log on to the RAMP GUI.
2. Upload the certificates obtained from the IdP and service provider (RAMP) one by one. Uploading the service provider certificate is optional. To generate a service provider certificate, refer to [Configure SAML Authentication](#).
 - a. Navigate to **MANAGEMENT > Authentication & Authorization > Certificates**.
 - b. Click **Add Certificate**. The "Add Certificate" window displays.

- c. Enter the **Alias Name**. If the alias name contains uppercase characters, it is automatically converted to lower case.
- d. Browse the certificates and upload.
- e. Click **Save**. The certificate is listed among the certificates.
3. Add a security realm for SAML:
 - a. Navigate to **MANAGEMENT > Authentication & Authorization > Security Realms**. Click **Add Security Realm**.
 - b. Enter a name for the realm in **Security Realm Name**.
 - c. To implement multi-tenancy, select a [tenant](#) for the realm from the **Tenant** list. The security realm is assigned to the root tenant by default.
 - d. Set the values in the **SAML Realm Properties** pane:

Parameter	Description
Identity Provider Certificate	The certificate provided by the IdP to validate the signature. Upload the IdP X.509 certificate for the SAML realm.
Service Provider Certificate	The certificate in RAMP used for decrypting the encrypted SAML assertion. Uploading a service provider certificate is optional. To generate a service provider certificate, refer to Configure SAML Authentication .
Returning Attribute	The name of the attribute to retrieve the user group from the SAML token. Set the same value as the name of the group attribute in the IdP configuration. The value is set to "UserGroup" by default.

- e. Click **Save**. The security realm for SAML is added.
4. Enable the SAML security realm to use it. Toggle the **Realm Status** button against the SAML realm to **Enabled**.
5. To set SAML as the primary authentication method on RAMP, refer to [Set Order of Priority for Authentication Methods](#). The users authenticated with external authentication methods including SAML are listed in the RAMP GUI: **MANAGEMENT > Authentication & Authorization > Users > External Users**. The count of tokens listed for each user indicates the number of active sessions. If the token count is not zero, it indicates the user is logged in.
6. To disable SAML authentication, navigate to **MANAGEMENT > Authentication & Authorization > Security Realms** and disable the SAML realm.

Generate Service Provider Certificate

To encrypt and decrypt SAML, you need a service provider certificate. Use the following procedure to generate the service provider certificate.

Start

1. Log on as `root` user.
2. Generate a certificate signing request:

```
openssl req -new -key /opt/sonus/auth/config/secure/auth_key.pem -out
certificate.csr
```


3. Generate and sign the service provider certificate using the generated certificate signing request and the same service provider private key `auth_key.pem`

```
openssl x509 -req -days 3650 -in certificate.csr -signkey /opt/sonus/auth/config/secure/auth_key.pem -out spcert.crt
```

Note

Upload the service provider (SP) certificate to RAMP and configure it with the SAML realm for the assertion decryption. Configure the same service provider at the IdP for encrypting the SAML assertion.

Configure Identity Provider

The Ribbon Application Management Platform (RAMP) allows you to set the `Group Attribute Statements` on the SAML settings of the Identity Provider (IdP).

Example of SAML setting from Okta IdP:

Single Sign On URL(Recipient URL/Destination URL)	<code>https://<RAMP-IP>/coreGui/ui/login/sso.jsp</code> Mandatory
Response	Signed
Mandatory	
Assertion Signature	Signed
Mandatory	
Assertion Encryption	Unencrypted/encrypted
Optional	
Group Attribute Statements	UserGroup
Mandatory	

Set the `Group Attribute Statements` on the SAML settings of the IdP.

Configure RADIUS Authentication

Ribbon Application Management Platform (RAMP) supports Remote Authentication Dial-In User Service (RADIUS) using the Password Authentication Protocol (PAP).

In the RADIUS security realm configuration, you specify the server IP address, server port, shared secret, number of retries, and request timeout settings. The RADIUS server also supports Network Access Server Identifier (NAS) if configured. The connection between RAMP and the RADIUS realm is established over User Datagram Protocol (UDP) using the hostname and port number configured in the RADIUS security realm. The shared secret password is encrypted and used for authenticating into the RADIUS realm. If the time taken to establish a connection between RAMP and the RADIUS security realm reaches the configured request timeout limit, then RAMP stops trying to reconnect. The RADIUS server authentication attempts are based on the configured number of retries. If the authentication or connection fails, or if the server is down, the RAMP raises

the trap [ribbonRadiusAuthServerUnreachable](#). When the server is up and the connection is established and authenticated, then RAMP raises a clearing trap [ribbonRadiusAuthServerReachable](#).

The RADIUS authentication process:

Step	Action	Description
1	Authentication Request	The user (client) initiates the authentication process by sending an authentication request to the RAMP.
2	Forward Request to Authentication Server	RAMP forwards the authentication request to the RADIUS authentication server.
3	Process Request and Authenticate User	The RADIUS authentication server processes the authentication request, validates the user credentials based on the database (or external authentication source), and authenticates the user.
4	Send Authentication Result to RAMP	After authenticating the user, if the returning attribute is set as VENDOR-DATA in RAMP, then the RADIUS searches in the RADIUS server and retrieves the value stored for VENDOR-DATA. The value returned must match the name of the usergroup defined in RAMP. If the user belongs to multiple user groups, then VENDOR-DATA returns multiple group names.
5	Forward Result to User	The RAMP forwards the authentication result to the user (client) that initiated the authentication request.

If one RADIUS server is unavailable, RAMP tries connecting to the next RADIUS server available in the sequence. To prioritize or set the sequence of the servers, refer to [Set Order of Priority for Authentication Methods](#). As a fallback mechanism for the RADIUS server, if you want local authentication on RAMP, then to configure local authentication, refer to [Configure Local Authentication](#).

Note

RAMP does not support CHAP (Challenge Handshake Authentication Protocol), EAP (Extensible Authentication Protocol), and accounting.

PAP, CHAP, and EAP authentication protocol is commonly used by Point-to-Point Protocol (PPP) servers, two machines that are directly linked communicating over the data link layer.

RADIUS is an open-standard Authentication, Authorization, and Accounting (AAA). Accounting is responsible for recording the activity of the user while they are connected to the network resource.

Prerequisites

- **Realm Administration** [privileges](#) under **Authentication and Authorization**.
- A user group is created in RAMP. For more information, refer to [Add User Groups](#).
- On the RADIUS server, update the configuration files with the user name, user groups, host name, and shared secret. For more information, refer to [RADIUS Administration](#).

Start

Create a guest user using this procedure to test the connection. Once you receive the success message, configure the RADIUS authentication.

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > Authentication & Authorization > Security Realms**.
3. Click **Add Security Realm**.
4. Configure the parameters and click **Save**.

Parameter	Description	Range
Realm Details		
Security Realm Name	Provide a unique name for the security realm.	1-256 characters.
Type	Select RADIUS as the realm type.	◦ LDAP ◦ SAML ◦ RADIUS
Tenant	Used to implement multi-tenancy. The default value is "root". For more information on multi-tenancy, refer to Configure Multi-Tenancy .	N/A
Radius Realm Properties		
Server IP Address	The IP address of the RADIUS server. It supports IPV4 and IPV6.	N/A
Server Port	The port number used to connect to the RADIUS server. The default port number is 1812.	N/A
NAS Identifier (optional)	(Optional) The NAS routes authentication requests to the RADIUS server.	
Shared Secret	This is a case sensitive character string configured on the RADIUS server for the RAMP IP and the same key is configured in the security realm in RAMP.	1- 256 characters.

Parameter	Description	Range
Returning Attribute	Name of the user group configured in the <code>users</code> file as VENDOR-DATA. This attribute returns the <code>usergroup</code> for RAMP. If the returning attribute is set as VENDOR-DATA, then the RADIUS searches in the RADIUS server and retrieves the value stored for VENDOR-DATA. The value returned must match the name of the <code>usergroup</code> defined in RAMP. If the user belongs to multiple user groups, then VENDOR-DATA returns multiple group names. RAMP checks if the returned <code>usergroup</code> is available in the local database and determines the role of the user. VENDOR-DATA is the Vendor Specific Attribute (VSA) name configured in <code>/opt/rbbn/auth/config/default_dictionary</code>. The default value is VENDOR-DATA. You can change the default value to any other name. Ensure the VSA name is identical to the returning attribute configured against the security realm. Refer to, Configure VSA.	N/A
Number of Retries	Set the number of times to retry connecting to the RADIUS server if the connection fails. The default value is 2.	0 to 10.
Request Timeout	If unable to connect to the RADIUS server, set the request time in seconds. The default value is 4.	1 to 30.
Test Connection	Click Test Connection to check if the connection is successful. A success message is displayed if the connection is successful.	N/A

5. Enable the RADIUS realm For more information, refer to [Enable or Disable Security Realms](#).

You can drag and drop to reorder the sequence of the RADIUS realm. For more information, refer to [Set Order of Priority for Authentication Methods](#).

RADIUS Administration

The Ribbon Application Management Platform (RAMP) supports user authentication through Remote Authentication Dial In User Service (RADIUS). Use this procedure to administer the RADIUS server.

Configuring RAMP on the RADIUS Server

To configure the RAMP on the RADIUS server:

1. From the RADIUS server, edit the `clients.conf` file by adding the RAMP IP address in order to accept requests from RAMP.

```
client 10.54.48.95/32 {
    secret          = radius123
    shortname       = test1
}
```

2. Add the user name and password in the `users` file as displayed in the following example.

Note

The VENDOR-DATA "value" (test) must be the *RAMP User Group Name* under which the user `test` is available.

```
test    User-Password := "test"
        Reply-Message := "User successfully Authenticated",
        VENDOR-DATA = "test"
```

3. Disable the system based authentication in `users` file as displayed in the following example:

```
# First setup all accounts to be checked against the UNIX /etc/passwd.
# (Unless a password was already given earlier in this file).
#
#DEFAULT          Auth-Type = System
#                Fall-Through = 1
```

4. Configure the vendor specific attributes in the `dictionary` file as displayed in the following example:

```
VENDOR          sonus          2879
BEGIN-VENDOR    sonus
#ATTRIBUTE      VENDOR-TYPE    1          integer
ATTRIBUTE      VENDOR-DATA     1          string
#VALUE          VENDOR-TYPE    VENDOR-SONUS 1
END-VENDOR      sonus
```

5. Start the RADIUS server as displayed in the following example:

```
[root@sbxlinux1 ~]# radiusd -X
Starting - reading configuration files ...
reread_config: reading radiusd.conf
Config: including file: /etc/raddb/proxy.conf
Config: including file: /etc/raddb/clients.conf
Config: including file: /etc/raddb/snmp.conf
Config: including file: /etc/raddb/eap.conf
main: prefix = "/usr"
```

Configure VSA

Use the following procedure to change the RADIUS security realm's **Returning Attribute** field by configuring a Vendor Specific Attribute (VSA) in `/opt/rbbn/auth/config/default_dictionary`

Start

1. Log on to the RAMP CLI as an `admin` user.
2. Change to insight user:

```
su - insight
```

3. Navigate to the `default_dictionary` directory:

```
vi /opt/rbbn/auth/config/default_dictionary
```

4. The default value is VENDOR-DATA. You can change the default value to any other name.

Example for changing VENDOR-DATA in default dictionary:

VENDOR	sonus	2879	
BEGIN-VENDOR	sonus		
#ATTRIBUTE	VENDOR-TYPE	1	integer
#ATTRIBUTE	VENDOR-DATA	1	string
ATTRIBUTE	VENDORDATA	1	string
#VALUE	VENDOR-TYPE	VENDOR-SONUS	1
END-VENDOR	sonus		

Note

If you rename the VENDOR-DATA attribute, update the same name in the security realm by logging on to the RAMP GUI after RAMP restarts.

Note

Ensure that the Attribute ID in the RAMP `default_dictionary` and the RADIUS dictionary is the same.

5. Restart RAMP for the VSA changes to take effect:
 - a. Stop the RAMP. For more information, refer to [How to Start and Stop RAMP](#).
 - b. Start the RAMP. For more information, refer to [How to Start and Stop RAMP](#).

Set Order of Priority for Authentication Methods

The Ribbon Application Management Platform (RAMP) executes the authentication methods it uses to authenticate users in order. If RAMP is unable to authenticate the user using the first method, it continues to the next until authentication succeeds or the methods are exhausted. Each method must have a configured security realm.

You can reorder the sequence in which security realms/authentication method are executed. Use the **Security Realms** window to arrange the sequence.

Disabled realms are ignored in the sequence during multi-realm authentication.

Prerequisites

- **Realm Administration** [privileges](#) under **Authentication and Authorization**.
- At least two security realms are available in RAMP.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > Authentication & Authorization > Security Realms**. The **Security Realms** window displays.
3. Click and drag the icon  up or down to change the realm sequence.

Enable or Disable Security Realms

The Ribbon Application Management Platform (RAMP) allows you to enable or disable the existing security realms. The security realm is disabled by default. Enable the security realm for user authentication (Users are authenticated only with enabled security realms).

A user cannot disable the local security realm.

Prerequisites

You require **Realm Administration** [privileges](#) under **Authentication and Authorization** for Enabling or Disabling Security Realms.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Security Realms**. The "Security Realms" window displays.
3. From the list of security realms, select the Realm you want to enable or disable.
4. From the "Realm Status" column, use the toggle control to enable or disable services.

Locations

In this section:

- [View SSH Key](#)
- [Create a New Location to Save the SSH Key](#)
- [Sync SSH Key](#)

The Ribbon Application Management Platform (RAMP) allows you to view and export SSH Keys to a new location on an external server.

If RAMP is upgraded or the SSH Key is regenerated, then RAMP allows replicating the new SSH Key onto all the external servers.

Note

If you want to add a location for Ribbon Analytics (RA), include the RAMP's `insight` user's `/opt/sonus/ems/.ssh/id_ecdsa.pub` key in RA using the RA GUI instead of adding it using the RAMP "Authentication and Authorization" GUI.

For more information, refer to [Configuring Ribbon Insight EMS Devices](#).

Prerequisite

User and **Role Administration** privileges in **Authentication and Authorization**.

View SSH Key

Perform the following procedure to view an SSH Key.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Locations**. The **Locations** window displays.
3. Click the ellipses (three vertical dots) menu and select **View SSH Key**.
4. The SSH Key window displays.

Create a New Location to Save the SSH Key

Create a new location to save the RAMP SSH Key on an external server in order to enable `passwordless` logins to that server from RAMP, as well as export PM statistics using SSH keys.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Locations**. The **Locations** window displays.
3. Click the **+ Add Location**. The **Add Location** window displays.
4. Update the details using the following table, and click Save.

Add Location Parameters

Parameters	Details
Name	The name of the location or server
IP Address	The IP address of the external server
User name	The user name to access and create a storage location on the server
Password	The password to access and create a storage location on the server

Sync SSH Key

When you upgrade RAMP or generate a new SSH Key, use this procedure to sync the SSH key onto the external storage location.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Management > Authentication & Authorization > Locations**. The **Locations** window displays.
3. Click on the (three vertical dots) menu and select **Sync SSH Key**.
Once the new SSH Key is copied to all the external storage locations, a success message is displayed.

Manage Certificates

You can upload and delete certificates for the Authentication and Authorization service using the Ribbon Application Management Platform (RAMP) GUI.

Prerequisites

User and Role Administration [privileges](#) under **Authentication and Authorization**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > Authentication & Authorization > Certificates**. The **Certificates** window displays.
3. To upload a certificate:
 - a. Click **Add Certificate**. The **Add Certificate** window displays.
 - b. Enter the **Alias Name**. If the alias name contains uppercase characters, it is automatically converted to lower case.
 - c. Browse the certificates and upload.
 - d. Click **Save**. The certificate is listed among the certificates
4. To view certificate details, click on a certificate in the **Certificate Alias** list.
5. To delete a certificate, perform one of the following:
 - a. To delete an individual certificate:
 - i. Click the delete icon under "Actions" for the certificate.
 - ii. Click **Yes** to confirm.
 - b. To delete multiple certificates:
 - i. Select multiple certificates.
 - ii. From the "Bulk Action" menu, select "Delete."
 - iii. Click **Yes** to confirm.

Importing Third Party Certificates

Use the following procedure to import third-party certificates and upload them to the Ribbon Application Management Platform (RAMP).

Prerequisite

User and Role Administration [privileges](#) under Authentication and Authorization.

Start

1. Logon to the RAMP GUI.
2. Navigate to **MANAGEMENT > Authentication & Authorization > Certificates**. The **Certificates** window displays.
3. To upload a certificate:
 - a. Click **Add Certificate**. The **Add Certificate** window displays.
 - b. Enter the **Alias Name**.

The alias name is automatically converted to lowercase if it contains uppercase characters.

- c. Locate and upload the certificates from your local machine.

When a Certificate Authority (CA) signs the certificate, import both the signed certificate along with the CA certificate into the RAMP for optimal authentication using certificates. If not, authentication into RAMP with a third-party certificate will not work.

- d. Click **Save**. The certificate is listed in the certificate list.
4. Add a User with the same name as the value in the **Common Name** for the certificate. To create a user name, refer to [Add Users](#).

To view the **Common Name** of the certificate:

- Navigate to **MANAGEMENT > Authentication & Authorization > Certificates**. The **Certificates** window displays.
- Click the certificate alias name. The certificate details are displayed.
- The **Subject Details** section displays the **Common Name** of the certificate.

Monitor User Activity

Ribbon Application Management Platform (RAMP) keeps a log of actions users perform when they are logged into the system. A RAMP administrator can monitor this activity by reviewing the logs.

The log provides advanced search options to locate specific types of entries. Note that the results include all records that meet the criteria and may take significant time to display. Ribbon recommends that you use the search criteria settings, especially **System Interval**, to limit the number of resulting records.

Prerequisites

User and Role Administration [privileges](#) in **Authentication and Authorization**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > Authentication & Authorization > Activity**. The **Activity** window displays.
3. Click **Advanced Search** to open the advanced search options you can use to filter the list.

Terminate User Sessions

A Ribbon Application Management Platform (RAMP) administrator can immediately terminate any active user session (HTTP or SSH). You might use this feature if system maintenance issues arise requiring the termination of all sessions except the administrator performing the maintenance, or if a particular user's access needs to be restricted or deleted.

Privileges

Super User [privileges](#) in **Insight Administration**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > User Sessions**. The **User Sessions** window displays.
3. Check the **Select** checkbox next to the user or users whose sessions you want to terminate.
4. Click **Terminate**.

Set Session Expiry in RAMP GUI

A Ribbon Application Management Platform (RAMP) administrator can set the expiry interval for user sessions on the RAMP GUI. After a set interval, users logged in to the GUI are automatically logged out and have to log in again.

Prerequisite

Super User [privileges](#) in **Insight Administration**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > Session Expiry**. The **Session Expiry** window displays.
3. Select the **User Session Inactivity Timeout** checkbox and enter an interval in minutes. The valid range is 5 to 120.
4. Click **Save**.

Authentication and Authorization Administration

Use the Ribbon Application Management Platform (RAMP) Device Management's **Administration** window to specify options that tailor the **Authentication & Authorization** service operations to your specific environment.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > Authentication & Authorization > Administration**.
3. Reference the following table when configuring the parameters, and click **Save** once done.

Authentication & Authorization Administration Parameters

Parameter	Length/Range	Description	Mandatory
Authentication Token Expiration			
Number of minutes before tokens expire	5 to 15 min	This specifies the validity period of the JWT token. By default, it is 15 minutes.	Y
User Activity Configuration			
Purge Frequency	1 to 7	The frequency of purge task that cleans-up the old User Activity Audit records. By default, the value is 1 (Represents everyday)	Y
Purge Start Time	Date (In 12-hour format)	Specifies the time to run the user activity purging task. By default, the value is 12:00 AM	Y
Purge before	1 to 365	The maximum number of days that a user activity audit record is to be stored in the database. By default, the value is 90 days.	Y
Password History Purge Configuration			
Password Purge Frequency	1 to 7	The frequency of purge task that cleans-up the old user password history change records. By default, the value is 1 (Represents everyday)	Y
Password Start Time	Date (In 12-hour format)	Specifies the time to run the user password history purge task. By default, the value is 12:00 AM	Y
Password Purge Before	1 to 3650	The number of days that a user password history record is to be stored in the database. NOTE: Ensure the value is not less than Password not reusable time period and Password Aging threshold set in Local Realms. By default, the value is 180.	Y

Parameter	Length/Range	Description	Mandatory
Certificate Expiration			
Number of days for certificate expiry notification	15 to 365	Specifies the number of days prior to certificate expiration to elapse before sending the notification. By default, the value is 15.	Y

EdgeView Service Administration

You can enable **EdgeMarc SIP Statistic Collection** on the Ribbon Application Management Platform (RAMP) to collect SIP statistics data from the EdgeMarc devices.

Prerequisites

Deploy the EdgeView Service on RAMP. For more information, refer to [Deploy Optional Services on RAMP](#).

Perform the following procedure to enable **Enable EdgeMarc SIP Statistic Collection**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > Edge View Service Administration**.
3. Enable **EdgeMarc SIP Statistic Collection**.

EdgeMarc SIP Statistic Collection status	Registered EdgeMarc Devices	Registering EdgeMarc Devices
On	If the EdgeMarc SIP Statistic Collection is changed from Off to On: • Push configuration is initiated to Enable SIP Statistics on all the registered devices. • Request EdgeMarc SIP statistics report from device on the next heartbeat.	The EdgeView service performs the following on the registration of an EdgeMarc device: • Request EdgeMarc SIP statistics report from the device. • Push configuration is initiated to Enable SIP Statistics on the device.

EdgeMarc SIP Statistic Collection status	Registered EdgeMarc Devices	Registering EdgeMarc Devices
Off	If the EdgeMarc SIP Statistic Collection is changed from On to Off: • Push configuration is initiated Disable SIP Statistics on all the registered devices. • Does not request the EdgeMarc SIP statistics report from device on the next heartbeat.	The EdgeView service performs the following on the registration of an EdgeMarc device: • Push configuration is initiated to Disable SIP Statistics on the device. • Does not request EdgeMarc SIP statistics report from device.

License Management

In this section:

- [Licensing Models](#)
 - [Node-Locked Licensing](#)
 - [Steps for Migrating from NWL License Mode to NWDL License Mode](#)
 - [Post-Paid Billing](#)
- [Planning for License Management](#)
- [Installing Licenses](#)
- [Associating Licenses with Devices](#)
 - [Node-Locked Licenses](#)
 - [NWDL Licenses](#)
 - [Licensing Profiles](#)
- [Monitoring License Status and Usage](#)
 - [Alerts for License Expiry](#)
 - [Generating Manual Reports](#)
- [Usage Reports for Post-Paid Billing](#)

Related articles:

- [License Management Workflows](#)
- [Find License Keys for Obtaining Licenses](#)
- [Obtain Licenses](#)
- [Install Licenses](#)
- [Activate Licenses](#)
- [Revoke Licenses](#)
- [Set Alerts for License Expiry](#)
- [Set Up Reporting for Post-Paid Billing](#)
- [Monitor License Usage](#)
- [Licensed Feature on RAMP](#)

The Ribbon Application Management Platform (RAMP) License Management (LM) service enables managing licenses for the Ribbon devices registered with it and for RAMP itself. The following sections overview general licensing concepts and RAMP's license management capabilities. However, it is always best to consult with your Ribbon account team for specific information on the licensing options available for your deployment and the requirements for license renewal or usage reporting that apply.

Licensing Models

Ribbon devices support two licensing models: node-locked licensing and network-wide domain licensing (NWDL).

Few devices use the NWL (Network Wide License) model, which is being deprecated. The NWL licenses were supported by the EMS, which could dynamically allocate them to the PSX or SBC device by tying them to their fingerprint.

Node-Locked Licensing

The RAMP License Management service manages node-locked licenses for devices operating in node-locked license mode. Node-locked is the traditional licensing method that ties the licenses to a specific host identifier or Virtual Machine Universal Unique Identifier (UUID).

For this model, when you request the required license files, you must provide the node-locked license key from the RAMP instance used to manage these licenses. This node-locked license key is used to create valid licenses. This “locks” the licenses to the LM service on the RAMP instance that provided the key. Once the license is subsequently installed on that RAMP instance, the licenses become available to associate with specific devices.

Though SBC Core and SLB devices support the node-locked licensing model, the node-locked licenses for these devices are derived from the devices' UUID (not from the RAMP's UUID) and then installed directly on the devices themselves. Furthermore, these licenses are not managed by the LM service.

Network-Wide Domain Licensing (NWDL)

The RAMP LM service manages NWDL licenses for devices operating in domain-locked (NWDL) license mode. In the NWDL model, licenses are associated with a domain or network instead of individual devices. This makes NWDL well-suited for deployments where the number of nodes is flexible and where nodes are added or removed more frequently. The Domain is defined as a single RAMP deployment and all devices registered and reporting statistics to that RAMP deployment. A RAMP deployment only has One Domain. Because of the flexible nature of the license association, NWDL deployments must participate in license usage reporting so that actual usage is reconciled with purchased licenses through the post-paid billing process.

When you request the required license files for this model, you must provide the domain-locked license key from the RAMP instance used to manage these licenses. This domain-locked license key is used to create valid licenses. The domain-locked license key is the public key of a private/public key pair generated by the LM service to ensure that only valid licenses (generated with the appropriate public key) are installed. Before installing them, the LM service verifies all NWDL licenses against its private key.

From the RAMP 23.09 release onwards (after the EMS migration to RAMP), the NWDL license counts and association details display when you select a PSX, SBC, or SLB node.

Steps for Migrating from NWL License Mode to NWDL License Mode

- The RAMP supports installing and associating NWL (Network-Wide Licensing) but does not allow reporting of NWL License usage in post-paid reports to the Ribbon Audit Portal (RAP).
- NWDL is supported only from PSX 15.1R0 release onwards on the KVM, VMware, RHV and CNe platforms.
- NWDL is supported on the OpenStack platform from release SBC 11.2 onwards.
- The AWS PSX platform does not support NWDL licenses. During a RAMP migration when the PSX and/or SBC elements use NWL and are on releases where NWDL is not supported, usage data is not collected and transferred to RAP. Due to this, time has to be limited.
- EMS customers using NWL licenses will have to relocate to RAMP, install NWDL licenses and associate NWDL licenses to the managed devices.

High Level General Upgrade path/procedure from NWL to NWDL

1. Pre-Migration
 - a. Contact Ribbon sales and verify that the Ribbon Audit Portal (RAP) collection is occurring and examine the NWL statistics.
2. During Migration
 - a. The RAMP manages PSX 14.1.x or 13.2.x along with the SBC 10.x or 9.x releases.

Complete the migration process as soon as possible to minimize license usage data getting lost.

- b. PSX upgrades from 13.x to 15.x directly are not supported. You must first upgrade from 13.x to 14.x, and then you can upgrade to 15.x or 16.x.
- c. SBC Core upgrades from 9.x to 12.x directly are not supported. You must first upgrade from 9.x to 10.x before you can upgrade to 12.x.
- d. Generate and Install the NWDL licenses on RAMP. For more information on generating licenses, refer to [Obtain Licenses](#). For more information on Installing licenses, refer [Install Licenses](#).
- e. Associate the NWDL licenses from RAMP to SBCs/ PSXs. For more information, refer to [Associate NWDL Licenses](#).
- f. Change the license mode from NodeLocked to Domain Locked on one of the OAM nodes, and then it gets pushed out to the service nodes while the changes are saved to the RAMP.
- g. For more information, refer to [Find License Keys for Obtaining Licenses](#).
- h. At this stage, the devices run the call in Domain Locked mode. The RAMP collects the usage stats from PSX and SBCs and reports it to NWDL usage to RAP in postpaid reports. For more information, refer to [Set Up Reporting for Post-Paid Billing](#).

Post-Paid Billing

Deployments that use NWDL licensing must regularly report usage to Ribbon as part of the post-paid billing process. To enable post-paid billing, RAMP must be licensed to generate license audit reports (RAMP_LIC_AUDIT_REPORT) for its managed devices. The RAMP license must also include either the manual (RAMP_LIC_MANUAL_REPORT) or automatic (RAMP_LIC_AUTO_REPORT) reporting feature as determined during the consultation with the Ribbon account team.

The LM service uses statistics collected by the Performance Management (PM) service to determine the actual usage across the network so that it can be sent daily, either automatically or manually, to a cloud-based billing system hosted by Ribbon IT (called the Ribbon Audit Portal or RAP). This session usage data is then reconciled

to billable invoices at the end of every cycle based on your contracted billing rates. The post-paid billing model applies only to NWDL licensing.

Refer to [Set Up Reporting for Post-Paid Billing](#) for information on setting up post-paid billing.

Planning for License Management

The choice of licensing model determines which licensing tasks are required for a deployment. In consultation with Ribbon personnel, you consider many characteristics of their deployment—size, node type, traffic patterns, platform, features required, and so on, to determine whether node-locked or NWDL licensing is more appropriate. Based on the model, you must obtain either the node-locked license key or the domain-locked license key from their RAMP instance prior to requesting licenses from the Ribbon Self-Service Licensing Portal so they can include the key with the license request.

For more information on obtaining the system license keys, refer to [Find License Key for Obtaining Licenses](#).

For more information on how to obtain a license file for a managed device, refer to [Obtain Licenses](#).

Installing Licenses

The RAMP LM service enables simple methods for installing Ribbon license files. To add licenses to the system, administrators can browse for a locally stored license file or drag and drop a file to install it. Ribbon license files are typically in an XML format. Administrators can also paste their XML license data directly into a window in the LM interface to add the license into the system. Note that for RAMP itself, once a valid license is installed, the features are automatically enabled on the system and no further action is required. However, for managed devices, the RAMP administrator must associate the installed license with the appropriate device.

For more information, refer to [Install Licenses](#).

Associating Licenses with Devices

After installing a license, the administrator associates the licenses with eligible managed devices. The process differs slightly based on the licensing model.

Node-Locked Licenses

A RAMP administrator associates node-locked licenses with registered devices operating in node-locked license mode, as needed, to support the features and capacity required on that specific device. You can disassociate a license from one device and associate it with another.

For more information on associating a node-locked licenses with devices, refer to [Associate Node-Locked Licenses](#).

NWDL Licenses

The RAMP administrator associates and enables the NWDL licenses on registered devices operating in domain-locked license mode. For counted feature licenses, the counts in the NWDL license represent the total count available for the entire domain (network). The administrator then associates per-node license allocations.

The same license allocation applies to all nodes in a cluster configuration. For an SBC cluster, the per-SBC-node allotment for each feature license is added to the cluster's configuration. This per-node allotment is then replicated to all SBC nodes in the cluster during configuration replication. All SBC nodes get identical license sets and counts.

For a PSX deployment, the per-node (replica) PSX allotment for each feature license is added to the PSX primary database. This per-node allotment is then replicated to all PSX nodes in the cluster as part of database replication. All PSX nodes get identical license sets and counts.

If either type of cluster expands to include another node, the same license allotment is automatically applied to the new node when it acquires its configuration from the cluster.

For more information on allocating and enabling the NWDL licenses, refer to [Associate NWDL Licenses](#).

Licensing Profiles

To assist with associating NWDL licenses, RAMP provides the option to create license profiles. A RAMP administrator can define a set of licenses in a profile and then assign the license profile to a cluster or to a registered node.

When a profile is assigned to a cluster, RAMP pushes the associated licenses to nodes automatically whenever nodes register with the cluster. License profiles enable an administrator to specify license associations in advance and associate them with a cluster when adding the cluster configuration to the system. If a node has a license profile assigned, the administrator cannot associate licenses with the node manually.

The same profile can be assigned to multiple clusters or to multiple registered nodes to ensure consistency in how licenses are applied. Refer to [Create and Assign License Profiles](#).

Monitoring License Status and Usage

To ensure their network devices have the necessary features and capacity available, RAMP administrators must monitor the status of their licenses to remain vigilant of the level of licensed feature usage. Administrators can monitor usage from two perspectives:

- **Per feature** — Use the *LM Feature Licenses list* to review the aggregate usage level of a selected feature license in either table or chart form. The LM service shows usage over a selected period compared to licensed capacity.
- **Per device** — Use the *LM License Association list* to monitor license usage on a per-device basis. From this list, an administrator can select a device and review the number of instances in use for each allocated feature compared to the number of instances allocated to the device.

For more information on monitoring license usage, refer to [Monitor License Usage](#).

Alerts for License Expiry

The LM service uses the LM Feature Licenses list to present a consolidated list of installed licenses, providing details such as the purchase order used to obtain the license and the date the license was generated. Above the license list, RAMP highlights the number of expired licenses and the licenses that will soon expire so administrators can quickly determine the overall license status.

In addition, RAMP generates an alarm to alert when a license is about to expire and again when a license expires. By default, RAMP generates the initial alert 14 days before a license expires. However, the administrator can choose a different global alert interval and configure overrides to apply intervals to specific licensed features.

For more information on license expiration alerts, refer to [Set Alerts for License Expiry](#).

Generating Manual Reports

The LM service offers multiple report options that enable RAMP administrators to gather license-related information in CSV, PDF, or XML format. This includes creating and saving report templates to produce customized reports. For example, reports can include detailed information on all licenses or a specific node or

license type. The administrator can immediately download or export reports to a specified destination or schedule them to run daily, weekly or monthly.

For more information on generating reports, refer to [Generate License Reports Manually](#).

Usage Reports for Post-Paid Billing

Customer deployments that use the NWDL licensing model must report their actual usage to Ribbon. When RAMP is licensed to generate license usage reports, it automatically generates daily usage reports on the managed devices. RAMP creates these reports daily at 1:00 AM system time using the previous day's usage data. The reports detail the license usage statistics at either a per-node level or at the entire network level for all installed feature licenses.

Sending this report to Ribbon is automatic or manual, depending on how RAMP is licensed.

- With automatic reporting, the LM service automatically sends daily usage reports to Ribbon.
- With manual reporting, the administrator must use the options provided in the LM interface to download and export the daily reports regularly to Ribbon.

For more information on submitting usage reports for post-paid billing, refer to [Set Up Reporting for Post-Paid Billing](#).

License Management Workflows

The following workflows outline the main steps required to complete key License Management tasks on Ribbon Application Management Platform (RAMP). Each step links to a page where you can obtain detailed information and procedures.

- [Installing and Associating Licenses](#) – install licenses and associate the licenses with specific managed devices.
- [License Usage Reporting](#) – generate reports to monitor your license usage or that enable the post-paid billing process.

Workflow – Installing and Associating Licenses

Step	Action
1	Obtain the RAMP license key needed to procure licenses you will manage with RAMP.
2	Procure the license file from Ribbon.
3	Install licenses on RAMP.
4	Associate licenses with devices.

Workflow – Creating and Associating License Profiles with Clusters

Step	Action
1	Obtain the RAMP license key needed to procure licenses you will manage with RAMP.
2	Procure the license file from Ribbon.
3	Install licenses on RAMP
4	Create a License Profile that specifies license allocations.
5	Include the License Profile in the cluster configuration.

Workflow – Creating and Associating License Profiles with Nodes

Step	Action
1	Obtain the RAMP license key needed to procure licenses you will manage with RAMP.
2	Procure the license file from Ribbon.
3	Install licenses on RAMP
4	Create a License Profile that specifies license allocations.
5	Associate the license profile with a node.

Workflow – License Usage Reporting

Step	Action
1	Generate license reports to obtain information on your license usage.
2	Configure license usage reporting for post-paid billing purposes.

Find License Keys for Obtaining Licenses

Each Ribbon Application Management Platform (RAMP) device contains unique license keys that identify it for license management purposes. Ribbon uses the license keys to identify the device (RAMP) authorized for managing the licenses. The licenses you obtain using a RAMP license key are tied to and managed by that RAMP device only. You cannot move or copy the license file to a different device.

When you request licenses, you must have the RAMP key for the type of license you are requesting: a node-locked license or network-wide domain license (NWDL). RAMP GR has two RAMP node-locked license keys and one domain-locked license key.

- When you generate node-locked licenses that you manage using RAMP, you must have the node-locked license key for your specific RAMP instance.
- When you generate NWDL licenses that you manage using RAMP, you must have the domain-locked license key for your specific RAMP instance. For post-paid billing, Ribbon uses the domain-locked license key in post-paid license reports to identify the RAMP device for billing.

For Ribbon licensing models, refer to [License Management](#).

Prerequisites

License Operations [privileges](#) in License Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management**.
3. Click the vertical ellipses and then click **Keys**.
The **Keys** dialog box displays.
4. Perform one of the following:
 - For node-locked licenses, copy the **RAMP Node Locked License key**. For RAMP GR, copy both values under **RAMP Node Locked License key**.
 - For NWDL licenses, copy the **Domain Locked License key**.

Obtain Licenses

Consult with a Ribbon-authorized sales representative to determine your licensing requirements. After placing a purchase order (PO) for licenses, you will receive an email from Ribbon with instructions for obtaining the license file.

The license generation process and feature IDs differ for node-locked and NWDL licenses. For the licensing models and feature IDs applicable for your device, refer to the device documentation.

For the Ribbon licensing models, refer to [License Management](#).

For Ribbon Application Management Platform (RAMP) licenses, refer to [Licensed Feature on RAMP](#).

Note

The instructions in this section apply if you are ordering and generating your license online. If your licensing is handled by your account team, contact them for ordering and generation.

The Ribbon Support Portal serves as the vehicle for delivering license bundles after the quoting and PO process is complete.

Prerequisites

The license keys are copied. To find the license keys, refer to [Find License Key for Obtaining Licenses](#).

Start

1. Consult with the Ribbon-authorized sales representative. You will receive an e-mail confirmation after placing the PO for licenses.
2. Follow the instructions in the e-mail to obtain the license file.
3. After obtaining the license file, install the licenses. For more information on installing the licenses, refer to [Install Licenses](#).

Install Licenses

After you use the Ribbon self-service licensing portal to [request a license](#), Ribbon emails a license file in XML format. A license file can include multiple feature licenses.

The contents of this file must be installed on the RAMP device that was the source for the license key used when generating the license. After you install the license, you can associate the license features with the devices registered with that instance of RAMP.

Note

RAMP can associate NWDL licenses to SBC 1000/SBC 2000 devices for versions 12.1 and above. License association is not applicable for SBC 1000/SBC 2000 devices with versions 12.0 and below.

License Installation

The following procedure explains how to install a license file.

Prerequisites

- License files are obtained from Ribbon. Refer to [Obtain Licenses](#).
- License Operations [privileges](#) in License Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > Feature Licenses**.
3. Click **Add License**. The **Add License** window displays.
4. Perform one of the following:
 - Click **Browse for file** and open the license file.
 - Copy the contents of the license file and paste it in the **Paste License Data Here** field.
5. Click **Save**. The license is installed, and the associated feature name is listed under **Feature Licenses**.

Activate Licenses

In this section:

- [Associate NWDL Licenses](#)
- [Create and Assign License Profiles](#)
- [Associate Node-Locked Licenses](#)
 - [Dissociate Node-Locked Licenses](#)

After you install a license file on Ribbon Application Management Platform (RAMP), the features within the license are available to associate with eligible devices that are registered on RAMP. Devices are eligible if they match the node type and license type for a feature license. Each registered device supports only one type of licensing model at a time. You can either associate node-locked or NWDL (domain-locked) licenses with a device, depending on the license mode set on the device. For NWDL licenses, you can create a license profile and use it to associate licenses with nodes or nodes in a cluster. Refer to [License Management](#) for a description of the licensing models.

Associate NWDL Licenses

If the license mode for a managed device is set as domain-locked, you can associate network-wide domain licenses (NWDL) with the device to use licensed features.

You can enable the same instance of the NWDL licensed feature on multiple devices by associating license counts with the devices. Every feature license has a max node limit available to be associated, which is set while generating the license. The maximum node limit defines the maximum number of license instances that can be enabled on a device. When you associate a count to a device, enable it to use the licensed feature. When you associate a count to a device, enable it to use the licensed feature. The associated count defines the level of usage allowed on the device. Set the value equal to or less than the maximum node limit value. If needed, the associated count can be modified in the future.

Billing for the feature is based on actual usage reported to Ribbon. To use post-paid licensing, refer to [Set Up Reporting for Post-Paid Billing](#).

Special Considerations for SBC Core and PSX

For pre 15.x PSX, the NWDL licenses can be associated only to the PSX Primary. These limits are then replicated to each PSX replica; both, the existing PSX replicas, and any new replicas which are instantiated subsequently. Enabling some of the PSX licenses may require base licenses in the right proportion.

For PSX 15.x and above, the NWDL licenses can be associated to the provisioning primary PSX or the primary PSX. License association is always redirected to the provisioning primary PSX, only this has read-write capabilities. The primary and replica PSX have read-only capabilities.

For SBC Core devices in cluster configurations, license configuration is set at the cluster level and then replicated among the devices. It is not necessary to configure each individual device in the cluster. For an N:1 OAM-based cluster, associate and enable the NWDL licenses only on the active OAM device. Instances Allocated count shows as 0 for SBCs associated with the OAM.

Note

Any installed NWDL licenses for the Ribbon Application Management Platform (RAMP) device itself are enabled automatically. You do not have to associate them manually.

Note

If a node has a license profile assigned, you cannot associate licenses with the node manually.

Note

RAMP can associate NWDL licenses to SBC 1000/SBC 2000 devices for versions 12.1 and above. License association is not applicable for SBC 1000/SBC 2000 devices with versions 12.0 and below. This is an existing functionality for SBC SWe Edge.

Prerequisites

- One or more license files are installed. Refer to [Install Licenses](#).
- The devices are registered on RAMP. Refer to [Registering Devices on RAMP](#).

- The license mode is set to NWDL on your device.
- You must have License Operations [privileges](#) in License Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > License Association**. The devices registered on RAMP are listed.
3. In the **Cluster or Single Node Name** column, click the device with which you want to associate NWDL licenses. The <device name> window displays.
4. Select the **NWDL** tab if necessary.
5. In the **Licenses associated or eligible to be associated with <device name>** pane, select a feature name.
6. Check the **Max Per Node Limit**, it is the maximum number of license instances that can be enabled on a device.

- If the license is not yet enabled on the device, the license status shows as "Ready."
- If the license is already enabled on the device, the license status shows as "In Use."

7. Enter the count of license instances to enable on the device in the **Current Associated Count** field.
8. From the **Bulk Actions** drop-down menu, click **Enable**. A dialog box displays to confirm.
9. Click **Yes**.
The following message displays
"Enable success"

Create and Assign License Profiles

In this section:

- [Create a License Profile](#)
- [Assign a License Profile to Nodes](#)
- [Edit a License Profile](#)
- [Copy a License Profile](#)
- [Delete a License Profile](#)

Related articles:

- [Create SBC Clusters](#)
- [Create PSX Clusters](#)
- [Create SLB Clusters](#)

You can create license profiles to assist with associating NWDL licenses with devices. To create a license profile, you specify a set of licenses and license counts for a specific type of device. To create a license profile, specify a set of licenses and license counts for a specific type of device, and then assign the profile to a cluster or to a registered node of the corresponding type.

To assign a license profile to a cluster, specify the profile in the cluster's configuration settings. With a license profile specified, no manual intervention is needed to associate licenses with individual nodes when they join the cluster. RAMP automatically pushes the specified licenses and license counts to nodes when they register with the cluster.

You can also assign license profiles to nodes that are not part of a cluster. For example, you can assign the same license profile to multiple nodes to ensure that you allocate license resources consistently. To assign a license profile to an individual node, ensure the node is already registered with RAMP.

Licensing profiles are applicable only for NWDL licenses and they are supported for SBC Edge, SLB, SBC Core and PSX devices only.

If a node has a license profile assigned, you cannot manually associate licenses with the node.

Note

RAMP can associate NWDL licenses to SBC 1000/SBC 2000 devices for versions 12.1 and above. License association is not applicable for SBC 1000/SBC 2000 devices with versions 12.0 and below. This is an existing functionality for SBC SWe Edge.

Create a License Profile

Create a license profile to specify a list of license and license counts you want to associate with a cluster or registered node.

Prerequisites

- License Operations [privileges](#) in License Management.
- NWDL licenses are enabled on your devices.
- NWDL licenses are installed on RAMP.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > License Profiles**.
3. Click **Add License Profile**. The **Add License Profile** window opens.
4. Use the following table to configure the profile.
5. Click **Save**.

Parameter	Description	Range
Name	A unique name for the license profile.	
Description	Optionally provide a brief description of the profile.	
Device Type	Select the type of device for which you are creating the license profile.	Select one of the following: • PSX • SBC Core • SBC Edge • SLB
License Instances	Select the license instances to associate with the profile. The list includes feature licenses available for the selected type of device. A profile must include at least once license instance. Enter the license count for the feature. The default value is the maximum limit available per device for the selected license.	

Assign a License Profile to Nodes

Use the following procedure to assign a profile to one or more nodes that are not part of cluster.

Prerequisites

A profile already exists.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > License Association**. The **License Association** window opens.
3. Select one or more nodes to which you want to assign the same profile.
4. Click the **Bulk Actions** menu. Select **Assign Profile**. The **Assign Profile** window opens.
5. From the drop-down for **License Profile**, select the profile.
6. Click **Save**.

Note

To assign a license profile to a cluster, you must specify the license profile in the configuration settings for a cluster. If a profile is part of the configuration of the cluster, RAMP automatically pushes the licenses specified by the profile to nodes in the cluster as they register. This is without manual intervention. Refer to [Create Clusters for Devices that Dynamically Register with RAMP](#).

Edit a License Profile

You can edit an existing license profile to update the licenses and license counts associated with the profile. Be aware that if you edit an existing profile that is assigned to a cluster or node, RAMP automatically updates the licenses associated with the nodes to align with the new values in the profile. If you do not want to update the license associations with the devices, you can use the copy procedure that follows to base a new profile on an existing profile.

Prerequisites

A profile already exists.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > License Profiles**
3. Select the profile to be edited. The **Edit Profile** page opens.
4. Select the **Feature Name** and update the **Current Associated Count**.
5. Click **Save**.
RAMP updates the licenses associated with devices to which the profile is assigned according to the new configuration.

Copy a License Profile

You can copy an existing license and save it with a new name with updated values.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > License Profiles**
3. Select the profile to duplicate. The **Copy Profile** page opens.
4. Update the **Name**, **Device Type**, **Feature Name** and the **Current Associated Count**.
5. Click **Save**.

Delete a License Profile

You can delete a profile if it is no longer needed and it is not associated with a cluster or node.

Prerequisites

The profile is not assigned to a device.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > License Profiles**
3. Select the profile to delete and click the Delete Profile icon in the **Actions** menu.
4. A confirmation message displays. Click **Yes**.

Associate Node-Locked Licenses

Related articles:

- [Dissociate Node-Locked Licenses](#)

If the license mode for a managed device is set as node-locked, you can associate node-locked licenses to your device to use licensed features. An instance of a node-locked feature license can only be associated to one device. When necessary, you can dissociate a feature license from one device to allow you to associate it with a different device. Refer to [Dissociate Node-Locked Licenses](#) for more information.

For PSX pre 15.x, CPS licenses associated to a replica can be used only by the replica, the same license cannot be used by its primaries or other replicas to process calls. To use the same license on a different node, the licenses have to be disassociated from the node and then associated to the other replica. Licenses applied to the primary PSX can only be used by the primary PSX in the primary cluster. Licenses applied to the replicas can only be used by the replica PSX in the replica cluster.

For PSX 15.x and above, node-locked licenses can be associated to the provisioning primary PSX or the primary PSX or the replica PSX. License association is always redirected to the provisioning primary PSX, only this has read-write capabilities. The primary and replica PSX have read-only capabilities.

Prerequisites

- One or more license files are installed. Refer to [Install Licenses](#).
- The devices are registered on RAMP.
- The license mode is set to node-locked on your device.
- Provisioner or Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- License Operations [privileges](#) in License Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > License Association**. The devices registered on RAMP are listed.
3. In the **Cluster or Single Node Name** column, click the device with which you want to associate node-locked licenses. The <device name> window displays.
4. In the **Node-Locked License Instances associated or eligible to be associated with <device name>** pane, select a feature name.

- If the license is not associated with any device, the license (feature name) shows as "Dissociated." You can associate the license.
- If the license is already associated with a device, the license (feature name) shows as "Associated." You cannot associate the license.

- From the **Bulk Actions** drop-down menu, click **Associate**. A dialog box displays to confirm.
- Click **Yes**.
The following message displays:
*"Success
Selected license instance(s) associated successfully"*

Dissociate Node-Locked Licenses

Related Topics:

- [Revoke Licenses](#)
- [Associate Node-Locked Licenses](#)

You can dissociate node-locked licenses from a device if they are no longer needed on that device. After dissociating a license, the license is available in Ribbon Application Management Platform (RAMP) so that you can associate the license with another device.

Prerequisites

- Provisioner or Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- License Operations [privileges](#) in License Management.

Start

- Log on to the RAMP GUI.
- Navigate to **MANAGEMENT > License Management > License Association**. The devices registered on RAMP are listed.
- In the **Cluster or Single Node Name** column, click the device name. The <device name> window displays.
- In the **Licenses associated or eligible to be associated with <device name>** pane, select a feature name.
- From the **Bulk Actions** drop-down menu, click **Dissociate**.
- Click **Yes** to confirm.
The following message displays
*"Success
Selected license instance(s) dissociated successfully"*

Revoke Licenses

You can revoke feature licenses that are no longer needed to remove them from the license inventory list. Revoking a license permanently removes it from Ribbon Application Management Platform (RAMP) and a device can no longer use the license. Both node-locked and NWDL licenses that are expired can be revoked. If it is not associated with any device, a node-locked license can also be revoked before it expires.

Prerequisites

- The license is not associated with a device.
- License Operations [privileges](#) in License Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > Feature Licenses**. The licenses installed on RAMP are listed.
3. In the **Feature Name** column, click the feature name. The **License Instances and Details** window displays.
4. Select a license.
5. Perform one of the following:
 - Click **Revoke** under the **Actions** column. A dialog box displays to confirm.
 - Select **Revoke** from the **Bulk Actions** menu. You can delete multiple licenses at once.
6. Click **Yes** to confirm.
A success message displays.

Set Alerts for License Expiry

Most licenses that Ribbon issues include an expiry date. If a feature license expires, the associated feature is disabled. To avoid this, you can configure expiration alerts so that you are notified before a license expires. You can specify individual alert intervals for specific feature licenses, if needed. Otherwise, a global alert setting applies to all feature licenses that are not individually configured.

You can view the count of licenses that are expired/expiring soon in the Ribbon Application Management Platform (RAMP) GUI, **License Management > Feature Licenses**.

Prerequisites

- Licenses are installed on RAMP.
- You must have License Management Administration [privileges](#) in License Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > Feature Licenses > Administration**.
3. In the **Instance Expiration** section configure the global alert setting by entering the number of days in advance you want to be notified when a feature license is about to expire.
4. Select the checkbox "Raise expiration alert traps" for RAMP to raise a [sonusLicStatusNotification](#) alarm when licenses are about to expire.
5. Click **Save**.
6. To set a separate limit for a specific feature license:
 - a. Navigate to **MANAGEMENT > License Management > Feature Licenses**. The licenses registered on Ribbon Application Management Platform display.
 - b. In the **Feature Name** column, click the feature name. The **License Instances and Details** window displays.
 - c. Select a license.
 - d. Click the <number of days> displayed against **Expiration Alert**. The dialog box **Expiration Alert Override** displays.
 - e. Select the radio button "Alert me day before expiration" and enter the number of days.
 - f. Click **Save**. A success message displays.

Set Up Reporting for Post-Paid Billing

Related articles:

- [Manually Upload Post-Paid Billing Reports](#)
- [Check Post-Paid License Usage](#)

The Network-Wide Domain Licensing (NWDL) model authorizes devices to process features/calls up to a specified burst limit or the actual physical capacity of the device. Deployments implementing NWDL must use post-paid billing to reconcile their usage with their purchased licenses. The post-paid billing process relies on Ribbon Application Management Platform (RAMP) regularly collecting usage data and reporting it to a cloud-based billing system hosted by Ribbon IT (called the Ribbon Audit Portal or RAP).

License usage data is collected as post-paid reports that RAMP generates every day. You can configure the RAMP to send the reports automatically, or an administrator can upload the reports manually.

The license usage data is plain-text JSON signed with a Ribbon key. Consequently, customers may directly view the information provided to verify correctness if necessary. To view post-paid reports, refer to [Check Post-Paid License Usage](#).

Note

From RAMP 23.12 onwards, SBC 1000/2000 license usage details are included in the post-paid reports.

Note

The RAMP registers to the Ribbon Audit Portal (RAP) using port 443. Ensure this port is enabled because the RAMP uses it when uploading post-paid reports.

Prerequisites

- Establish Reports Operations [privileges](#) in License Management.
- Ensure RAMP is connected to the internet.
- Ensure Devices using NWDL are registered with RAMP and the licenses are activated on the devices.
- The RAMP_LIC_AUDIT_REPORT license is installed.
- One of the following licenses is installed, based on whether you are using manual or automatic reporting:
 - RAMP_LIC_MANUAL_REPORT: The license to facilitate uploading post-paid reports manually. The RAMP administrator must manually transfer the post-paid reports to Ribbon for every billing cycle. To send post-paid reports manually, refer to [Manually Upload Post-Paid Billing Reports](#).
 - RAMP_LIC_AUTO_REPORT: The license to enable uploading post-paid reports automatically. The RAMP automatically transmits the post-paid reports to the Ribbon licensing portal. Automatic reporting eliminates the need for periodic customer action to reconcile license usage.

Start

1. Log on to the RAMP GUI.

Note

Skip Step 2 if you have installed RAMP_LIC_MANUAL_REPORT.

2. Establish connectivity between the [Ribbon IT portal](#) and RAMP if you have installed RAMP_LIC_AUTO_REPORT:
 - a. Navigate to **MANAGEMENT > License Management > Post-paid Reports**.
 - b. Click **Register**. After establishing the connection, the status message in *Connectivity with Ribbon IT* changes to *Registered* and *Connected*. For information on ports, refer to [RAMP Ports Descriptions](#).
3. Set options that determine how frequently RAMP collects usage statistics and how long it retains usage data. If you use automatic usage reporting, specify how RAMP interacts with the Ribbon IT system:
 - a. Navigate to **MANAGEMENT > License Management > Administration**.
 - b. Configure these parameters.

Parameter	Length/Range	Default	Description
LM Instance Expiration			
Alert Me			
Alert me <X> days before any feature license is set to expire.	N/A	14	The number of days to elapse before a license expires.
Raise expiration alert traps	N/A	Disabled	Enable to raise license expiration alerts based on your input in the above field.
LM Reports			
Reports			
Retain row data used in Reporting for	N/A	180	The duration, in days, to retain the data used for license reports. • 30 • 90 • 180 (Default)

Parameter	Length/Range	Default	Description
Generate NodeLevel PostPaid Reports	N/A	Disabled	- Enables the generation of node-level postpaid reports when the checkbox is selected. - Disables the generation of node-level postpaid reports when the checkbox is not selected. (default) Note: By default, the node-level postpaid reports are disabled and only the network-level postpaid reports are generated.
LM Management			
IT Retry			
Ribbon IT retries, count	1-5	2	The number of retries RAMP attempts when interacting with Ribbon IT if there are connectivity issues.
Ribbon IT retries, delay in seconds	1-20	5	The interval, in seconds, between retries when interacting with Ribbon IT.
License usage statistic retention, in days	1-90	30	The duration, in days, to retain the license usage statistics in the RAMP database. Any data older than the set duration is deleted.
License usage statistics collection	N/A	5	The frequency, in minutes, at which RAMP collects licenses usage statistics from PM statistics. Ensure it matches with the statistics collection frequency of the devices. 5 (Default) 15

Parameter	Length/Range	Default	Description
RAMP Alias	1-40	RAMP-0vhYbbGqbW	Provide an alphanumeric alias for RAMP. This helps to uniquely identify a particular RAMP on the billing server. The default value is RAMP -0vhYbbGqbW . Where, 0vhYbbGqbW is a system-generated random value.

- c. Click **Save**.
4. If the status displays Unregistered or Disconnected, ensure that your firewall settings allow connectivity from the RAMP to the Ribbon license reporting portal: callhome.rbbn.com. This link works only from REST API.

Note

Ensure that [port 443](#) is open.

Manually Upload Post-Paid Billing Reports

Some deployments are licensed to manually report license usage data. Ribbon Application Management Platform (RAMP) generates and saves daily license usage reports, but these reports must then be manually uploaded to Ribbon if your licensing specifies manual reporting. After consulting with a Ribbon-authorized sales representative on what is appropriate for your deployment, you can choose to upload Network-level or Node-level reports (in JSON format). These usage reports contain the following:

- Network Level reports - The usage details of licenses across the network in five-minute intervals for the past day.
- Node Level reports - The usage details of licenses per device in five-minute intervals for the past day.

This procedure describes how to manually upload post-paid billing reports.

Prerequisites

- You must have Reports Operations [privileges](#) in License Management.
- Post-paid licenses are restricted and not available for quoting directly, they require prior approvals from sales and product management.
- Post-paid licensing is configured with the feature RAMP_LIC_MANUAL_REPORT. For more information on configuring post-paid licensing, Refer to [Set Up Reporting for Post-Paid Billing](#).

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > Post-paid Reports**.
3. Perform one of the following:
 - To upload node-level reports, click the **Node Level** tab.
 - To upload network-wide reports, click the **Network Level** tab.
4. Select the reports.
5. From the **Bulk Actions** drop-down menu, click **Download / Export**.
6. Perform one of the following:
 - To download the report, select the radio button **Download** and click **Download**.

- To export the report, select the radio button **Export** and click **Export**.
- 7. A zip file is created with the selected reports in the location specified in download or export. You must now upload this zipped file to the **Ribbon** licensing portal.
- 8. Log on to the **Ribbon** licensing portal.
- 9. Navigate to the License **Usage** drop box.
- 10. Select the **Upload** option and specify the zipped file containing the reports.

Once the file is uploaded, a usage report is generated and sent to Ribbon. No further action is required

Monitor License Usage

In this section:

- [Generate License Reports Manually](#)
- [View Usage of NWDL Licenses](#)
- [View License Usage on a Device](#)
- [Check Post-Paid License Usage](#)

Ribbon Application Management Platform (RAMP) collects data on license usage by registered devices. You can check license usage by generating reports for individual licenses, across the network, or for a device.

RAMP does not manage or track license usage for licenses that are directly installed on the devices.

Generate License Reports Manually

The Ribbon Application Management Platform (RAMP) helps you keep track of the status of your feature licenses. You can audit your license inventory by generating license reports that provide details about the licenses in your network. When you generate a report, you can select the type of information you want to review:

- Types of licenses currently installed: node-locked or NWDL
- Availability and usage: installed, in use, and revoked
- Expiration status: safe, expiring soon, and expired
- Devices using these licenses: type and IP address

With information from a license report, you can:

- Check whether your licenses are expired or expiring soon.
- Determine which licenses you no longer need so you can remove them. To remove licenses, refer to [Revoke Licenses](#).
- Find the history of license purchase and activation.
- Compare license usage versus availability. Some of the license may be needed in larger quantity in your network and some licenses might be used sparingly. License reports help you optimize your license-buying strategy and with evaluating the effectiveness of your current licensing model.

Prerequisites

- You must have **Reports Operations** [privileges](#) in License Management.
- The **RAMP_LIC_AUDIT_REPORT** license is installed.

Note

RAMP provides a wide range of options to customize a report. When you add a report, parameters appear in four sections: **Report Details**; **License Details and Date Range**; **Report Columns**; and **Frequency Format and Location**. Many parameters are dynamic and the options available change as you make selections. The following procedure outlines the steps for each report type. Be aware that some options offered for one type of report may not appear or apply in a different report scenario.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > Manual Reports**. The **Manual Reports** window displays.
3. Click **Add Report**. The **Create Report** window opens.
4. Configure the options in the **Report Details** section:
 - a. Enter a name for the report in the **Report Name** field.
 - b. Enter a description of the report in the **Report Description** field.
 - c. Select one of the following **Report Types** and configure parameters that select data for the report:
 - **License:**
Select the **License** radio button, the **License** report type supports three sub-types:
 - **Summary:**
 - a. Select the licensing models.
 - b. Select the feature licenses.
 - c. Select the expiration status types.
 - **Instance:**
 - a. Select the licensing models.
 - b. Select the feature licenses.
 - c. Select an expiration date range.
 - **Historical:**
 - a. Select **Per License** to include data specific to a selected feature license. Select **Per Cluster** to include data is specific to a selected cluster.
 - b. Select the **Node Types** (per license) or **Cluster Name** (per cluster) to filter data.
 - c. Select one feature license (per license) or a set of feature licenses (per cluster) to include in the report.
 - d. Select an interval for the report.
 - **Node:**
 1. Select the **Node** radio button.
 2. Select node types.
 3. Select the specific nodes.
 - **Revoked:**
 1. Select the **Revoked** radio button.
 2. Select an interval for the report.
5. In the **License Details and Date Range** section:
 - a. Select the **License Type** from the list. The report is generated based on the type of license you select.
 - i. Select **All License Types** if you want to generate a report for both, NWDL and Node-Locked licenses.
 - ii. Select **NWDL** to generate only NWDL licenses.
 - iii. Select **Node-Locked** licenses to generate a report for Node-Locked licenses.
 - b. Select the **License To Include**. Based on the type of license selected in the previous step, the list licenses are listed.
 - c. Select the **Expiration**. You can select the license based on their date of expiry.
6. In the **Report Columns** section, use the **Available** and **Selected** columns to specify which data columns to include in the report. Use the arrows to move the columns you want to include into the **Selected** list. The columns appear in the order you list them.

7. Configure the options in the **Frequency, Format and Location** section:
 - a. Under **Frequency**, select a frequency for the report.
 - To generate the license report on demand, select **Now**.
 - To schedule the report to run at a later time:
 1. Select **Later**.
 2. Select a date.
 3. Select a time of day to run the report.
 - To schedule generating the report on a repeating basis:
 1. Select **Repeat**.
 2. Select the frequency at which you want to repeat running the report:
 - **Daily** – specify the time of day.
 - **Weekly** – specify the day of the week and time of day.
 - **Monthly** – specify the day of the month and time of day.
 - b. Under **Format**, select the format for the report: **CSV**, **PDF**, or **XML**.
 - c. If you configure the report to run immediately (**Now** option), you can choose to download the report or export it to a specified location. This choice applies only if you have specified the **Frequency** option as **Now**. Under **Download/Export**, select either the **Download** or **Export** option.
 For the other **Frequency** options (**Later** and **Repeat**) you must provide one or more export locations where RAMP can store the report at the scheduled time. Under **Export Locations** check **Localhost** if you want to export the report to a location on RAMP. If you want to export the report to a different server, enter an **IP Address**, **Directory** path for the report file, and a **Username** and **Password** to enable access to the destination server.
8. When you complete specifying the parameters for the report, click **Save**. If you configured the report to run now and to download, RAMP runs and downloads the report. For all other frequency and location options, RAMP runs the report when scheduled and stores the output in the specified location.

RAMP stores the report parameters under the **Report Name** you provided and adds the report to the list on the **Manual Reports** window. From the **Manual Reports** list you have the option to edit, run, or delete a stored report.

View Usage of NWDL Licenses

You can analyze your usage of NWDL licensed features by reviewing usage data over time. Ribbon Application Management Platform (RAMP) provides usage data in both tabular and graphic forms. You can retrieve the usage data of a feature license between 5 minutes to 5 days.

Prerequisites

- View Licenses and Reports [privileges](#) in License Management.
- NWDL licenses are enabled on your devices.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > Feature Licenses**. The licenses registered on RAMP display.
3. In the **Feature Name** column, click the feature name. The **License Instances and Details** window displays.
4. In the License Usage area, click **Chart View** or **Table View**.

Chart View

A graph is plotted with the count of licenses installed, average usage, and average usage in an interval. You can aggregate license usage on a daily or hourly basis, or both.

Keep your cursor on any of these items in the legend (defined on the x-axis), the corresponding data in the chart is highlighted with an outline.

- **Licenses Installed:** The total count of the license instances installed.
- **Average Usage:** The average usage count for the license instance.
- **Average Usage (Interval):** The average usage count for the license instance in the interval.

Keep your cursor in the chart area to view the absolute numbers for these items within an interval.

Table View

You can aggregate license usage on daily or hourly basis or both in the tabular view and view the following details:

- **Time:** The start time for the interval.
- **Status:** The status of the license based on the expiry date:
 - **Safe:** The license will not expire soon.
 - **Unsafe:** The license is about to expire.
- **Used:** The usage count for the license instance during the interval.
- **Installed:** The total count of the license instances installed.
- **Recent Peak:** The time at which the peak usage for the license observed.
- **Peak Usage:** The count of license instances used at the peak usage. If the license usage data shows peaked usage frequently, you may consider adding more licenses to avoid exhausting the licenses.

View License Usage on a Device

You can view licensed feature names, counts, and time of last usage for registered devices whose licenses are managed in Ribbon Application Management Platform (RAMP).

License usage data is based on the last successful collection of performance statistics. License usage for a device is reported only if performance statistics have been collected at least once, with values other than zero.

To view the license usage by a node, select the respective node in License Association on RAMP.

For RAMP redundancy, license usage data for all RAMP devices in a redundancy setup display collectively.

Prerequisites

View Licenses and Reports [privileges](#) in License Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > License Association**. The devices registered on RAMP display.
3. In the **Cluster or Single Node Name** column, click the device name. The <device name> window displays.
4. Perform one of the following:
 - For an individual node, click the name of the node. Feature licenses associated with <node name> window displays.
 - For a node within a cluster:
 - Click a cluster name. The names of all the nodes in the cluster display.
 - Click the name of a node. Feature licenses associated with <node name> window displays.

Check Post-Paid License Usage

The Ribbon Application Management Platform (RAMP) collects license usage statistics for post-paid billing. RAMP generates post-paid reports every day at 1:00 AM system time using the previous day's usage data.

RAMP generates the following reports:

Report	Description
Network Level report	Usage details of licenses across the network for the past day, as per the collection intervals configured in PM collection profiles.
Node Level reports	Usage details of licenses per device for the past day, as per the collection intervals configured in PM collection profiles.

Use the following procedure to check the post-paid reports to analyze license usage:

The Network level license post paid reports are enhanced with the addition of two columns , "PRIMARY-PSX-NODE-COUNT" and "REPLICA-PSX-NODE-COUNT", which list the registered online node count of primary and replica nodes.

Note

You can only download **Node Level Reports** and **Network Level Reports** in JSON and JSON/PDF/HTML formats, respectively.

From RAMP 23.12 onwards, the Network Level report and Node Level report includes the usage of SBC1000/SBC 2000 devices.

Along with license usage, the node platform details are also reported in the node level post paid reports.

Prerequisites

- Verify Licenses and Reports [privileges](#) in License Management.
- Verify Post-paid licensing is enabled. Refer to [Set Up Reporting for Post-Paid Billing](#).

Start

1. Log on to the RAMP GUI.
2. Navigate to **MANAGEMENT > License Management > Post-Paid Reports**.
3. Perform one of the following:
 - To view node-level reports, click the **Node Level** tab.
 - To view network-wide reports, click the **Network Node Level** tab.
4. Click on the report name. The Report window displays.
5. To download the report:
 - a. In the Download / Export section, select the **Download** radio button.
 - b. Select a report format from the **Report Format** list.
 - c. Click **Download**.
6. To export the report:
 - a. In the Download / Export section, select the **Export** radio button.
 - b. Select a report format from the **Report Format** list.
 - c. Perform one of the following:
 - To export the report to a directory on RAMP, select the **LocalHost** check-box.
 - To export the report to a remote location:
 1. Enter an IP address for the destination location.
 2. Enter a directory name.

3. Enter the username and password to access the destination.
- d. Click **Export**.

Licensed Feature on RAMP

The licensed features on the Ribbon Application Management Platform (RAMP) and the associated licenses are listed in the subsections. Generate RAMP licenses using either the Node Locked License or Domain Locked License keys. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#).

In this section:

- [Node Locked Licenses on RAMP](#)
- [Domain Locked Licenses on RAMP](#)

Node Locked Licenses on RAMP

In this section:

- [RAMP Licenses](#)
- [PSX Policy Server](#)
 - [PSX Policy Server Licenses](#)
 - [PSX SWe](#)
- [SBC Core \(5x10, 5400, 7000, and SWe\)](#)
- [MRFP Licenses](#)
- [DSI Licenses](#)
 - [DSI-HW Feature Licenses](#)
 - [DSI Licenses](#)
 - [DSI SWe](#)
- [SGX4000](#)
 - [SGX4000 Licenses](#)
 - [SGX4000 SWe](#)

In the traditional node-locked licensing model, licensing is tied to a host identifier. In a non-virtualized environment, the server hardware ID is used as the identifier. In a virtualized environment, the Virtual Machine (VM) UUID is used. For the both cases, the license is restricted to that particular server or VM, and that license file cannot be moved or copied onto a different instance.

Node-locked licensing for the SBC products is managed directly on the SBCs. The Ribbon Application Management Platform (RAMP) is not involved in distributing SBC node-locked licensing in any manner. For more information on managing SBC node-locked licenses, refer to the [Node-Locked Licensing](#).

Node-locked licensing for the RAMP functionality is managed by the RAMP. These RAMP node-locked licenses are associated with the host ID or UUID of the RAMP instances (active and GR). These licenses are installed on to the RAMP License Manager (LM) and used by the RAMP itself.

Node-locked licensing for the PSX products is also managed through the RAMP. The PSX node-locked licenses are also associated with the ID of the RAMP. First, these PSX node-locked licenses are installed on to the RAMP License Manager (LM). Next, subsets of these PSX licenses are assigned to specific PSX replicas registered

with the RAMP. The RAMP tracks the assignments and also allows the disassociation of licenses from specific PSX replicas.

This page lists Node Locked Licenses on the RAMP.

RAMP Licenses

The following RAMP licenses are generated using the Node Locked License key. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#). These licenses are listed on the RAMP as Node Locked.

License (Feature ID)	Description
RAMP-BASE	The licenses to use the RAMP standalone.
RAMP-BASE-GR	The licenses to use the RAMP GR.
RAMP-SSO	The licenses to use MFA/SSO functionality on the RAMP using SAML2.0 to customer's Identity Provider (IdP).
RAMP-LI	The licenses to use Lawful Intercept functionality on the RAMP.
NW-HPC	The licenses to use High Probability Completion (HPC) functionality across the Ribbon network (PSX and GSX). When upgrading an existing (pre-V08.00.00) system running HPC, avoid loss of HPC service by performing the following upgrade steps: • Upgrade the RAMP nodes. • Install and activate the HPC license (NWHPC). • Upgrade the PSX nodes. • Upgrade the GSX nodes.
NW-MLPP	The licenses to use Multilevel Precedence and Preemption (MLPP) functionality across the Ribbon network (PSXs and GSXs).
RAMP-LNP-FEED	The licenses to use Local Number Portability (LNP) functionality on the RAMP. The LNP functionality involves accepting and processing data feed on the RAMP which in turn provisions the primary PSX with the National Portability Administration Center (NPAC) LNP Data.
RAMP_LIC_AUDIT_REPORT	The license to generate license reports on the RAMP.
RAMP_LIC_MANUAL_REPORT	The license to generate post-paid license reports on the RAMP. The operator needs to manually download the license usage data and send it to Ribbon IT for billing. Note The RAMP_LIC_AUDIT_REPORT license is required to use RAMP_LIC_MANUAL_REPORT.

License (Feature ID)	Description
RAMP_LIC_AUTO_REPORT	The license to generate on RAMP and automatically send post-paid license reports to the Ribbon IT. Note The RAMP_LIC_AUDIT_REPORT license is required to use the RAMP_LIC_AUTO_REPORT license.

Note

RAMP-CORE-API and RAMP-CLI licenses are not mandatory to install on the RAMP for provisioning.

PSX Policy Server

These licenses are generated using the Node Locked License key. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#). These licenses are listed on the RAMP as Node Locked.

Note

All PSX licenses (except POLVPN and POLHSXSUB, which are based on the number of subscribers and POLSPE) are issued per CPU basis.

You need to associate the BASE license with the functional CPS licenses (CRS or Non-CRS, that is, Outbound or with both) to the PSX primary.

To enable only D+ CPS traffic, you can install the BASE license separately.

- Base count = D+ count + SIP count + ENUM SRV count.
- D+ count= Base count - (SIP count + ENUM SRV count).
- All outbound licenses count except for LCR = Base count.

PSX Policy Server Licenses

License	Description	Displayed on RAMP
H323PGKSW	This license provides H.323 Gatekeeper functionality on the Ribbon PSX Policy Server.	Node Locked
POLAINVPN	This license provides AIN Voice VPN functionality on the Ribbon PSX Policy Server. This license also requires the purchase of the ANSI TCAP license (POLTCAP).	Node Locked

License	Description	Displayed on RAMP
POLENUM	This license provides ENUM translation functionality through an LWRES (Light Weight Resolver Daemon) server installed locally on the PSX, which handles queries to an external DNS. Customers may perform DNS translation without a feature license, but the POLENUM feature license is required to perform ENUM translation.	Node Locked
POLGSM	This license provides functionality for GSM mobile services on the PSX.	Node Locked
POLHSXSUB	This license controls the maximum number of Subscribers you can provision to the HSX.	Node Locked
POLIN	This license provides IN CNAM Toll-Free functionality on the Ribbon PSX Policy Server. This license also requires the purchase of the ANSI TCAP license (POLTCAP).	Node Locked
POLIS41	This license provides IS41 functionality on the Ribbon PSX Policy Server and requires the ANSI TCAP license (POLTCAP) purchase.	Node Locked
POLITUTCAP	This license provides ITU TCAP functionality on the Ribbon PSX Policy Server. This license only supports GSM mobile services; it does not support any other ITU TCAP based services.	Node Locked
POLLNP	This license provides AIN LPN functionality on the Ribbon PSX Policy Server and requires the purchase of the ANSI TCAP license (POLTCAP).	Node Locked
POLSIP	This license provides SIP Core Proxy functionality on the Ribbon PSX Policy Server and SIP Redirector/ Application Server Interface functionality on the Ribbon PSX Policy Server.	Node Locked
POLSIPSCP	This license provides SIP-based SCP authorization code validation and external route server queries on the PSX.	Node Locked
POLSPE	This license provides SPE Script loading functionality on the Ribbon PSX Policy Server.	Node Locked
POLTCAP	This license provides ANSI TCAP functionality on the Ribbon PSX Policy Server.	Node Locked

License	Description	Displayed on RAMP
POLTESTDB	This license provides Test Data Access to the PSX database. Administrators can provision in an active production PSX database and conduct call processing testing without the changed data being applied to or otherwise affecting real-time network operations.	Node Locked
POLTF	This license provides AIN Toll-Free functionality on the Ribbon PSX Policy Server. This license also requires the purchase of the ANSI TCAP license (POLTCAP).	Node Locked
POLTRANS	This license provides Number Translation functionality on the Ribbon PSX Policy Server.	Node Locked
POLVPN	This license provides Voice VPN functionality on the Ribbon PSX Policy Server and controls the maximum number of VPN Subscribers that you can provision.	Node Locked
POL3RDPTYACCESS	This license supports SIP signaling to third-party Class 5 feature servers, as well as the standard PSX functionality (that is, numbering plans, routing, etc.) required to support these servers.	Node Locked
POLXMLAS	This license provides PSX support for third-party application servers through XMLOverTCP messaging on the Ribbon PSX Policy Server.	Node Locked
POL-LNP-STORE	This license on PSX supports LNP data storage on board for LNP local lookup instead of checking an external SCP.	Node Locked
POL-LCR-100CPS	This license provides VBR Functionality on Ribbon PSX Policy Server.	Node Locked

PSX SWe

These licenses are generated using the Node Locked License key. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#). These licenses are listed on the RAMP as Node Locked.

PSX SWe Licenses

License	Description	Displayed on RAMP
POL-SWE-BASE-SW-100CPS ¹	This license provides D+ functionality on the Ribbon PSX Policy Server. For ingress D+ traffic, this license allows a maximum of 100 Calls per second. This license also serves as Base License for CPS based licenses in the package.	Node Locked

License	Description	Displayed on RAMP
POL-SWE-BASE-SW-5CPS ¹	This license provides D+ functionality on the Ribbon PSX Policy Server. For ingress D+ traffic, this license allows a maximum of 5 Calls per second. This license also serves as Base License for CPS based licenses in the package.	Node Locked
POL-SWE-SIP-100CPS ¹	This license provides SIP functionality on the Ribbon PSX Policy Server. This license allows a maximum of 100 Calls per second for ingress SIP traffic. This license supports 100 CPS capacity to the PSX server.	Node Locked
POL-SWE-SIP-5CPS	This license provides SIP functionality on the Ribbon PSX Policy Server. For ingress SIP traffic, this license allows a maximum of 5 Calls per second. This license supports 5 CPS capacity to the PSX server.	Node Locked
POL-SWE-ENUMSVR-100CPS ¹	This license provides ENUM Gateway functionality on the Ribbon PSX Policy Server. For ingress ENUM traffic, this license allows a maximum of 100 Calls per second.	Node Locked
POL-SWE-ENUMSVR-5CPS ¹	This license provides ENUM Gateway functionality on the Ribbon PSX Policy Server. For ingress ENUM traffic, this license allows a maximum of 5 Calls per second.	Node Locked
POL-SWE-ENUMCLT-100CPS ²	This license provides ENUM functionality on the Ribbon PSX Policy Server. For Egress ENUM traffic, the license is of the same quantity as the BASE CPS License. This license supports 100 CPS capacity to the PSX server.	Node Locked
POL-SWE-ENUMCLT-5CPS ²	This license provides ENUM functionality on Ribbon PSX Policy Server. For Egress ENUM traffic, the license is of the same quantity as the BASE CPS License. This license supports 5 CPS capacity to the PSX server.	Node Locked
POL-SWE-IN-100CPS ²	This license provides IN - CNAM and LEC Toll-Free functionality on Ribbon PSX Policy Server. For egress IN - CNAM and LEC Toll-Free traffic, the license is of the same quantity as BASE CPS License. This requires the same quantity of POL-TCAP-100CPS licenses.	Node Locked

License	Description	Displayed on RAMP
POL-SWE-IN-5CPS ²	This license provides IN - CNAM and LEC Toll-Free functionality on Ribbon PSX Policy Server. For egress IN - CNAM and LEC Toll-Free traffic, the license is of the same quantity as BASE CPS License. This requires the same quantity of POL-TCAP-5CPS licenses.	Node Locked
POL-SWE-ITUTCAP-100CPS ²	This license provides ITU TCAP functionality on Ribbon PSX Policy Server. For egress ITU TCAP traffic, the license is of the same quantity as BASE CPS License. This license supports 100 CPS capacity to the PSX server.	Node Locked
POL-SWE-ITUTCAP-5CPS ²	This license provides ITU TCAP functionality on Ribbon PSX Policy Server. For egress ITU TCAP traffic, the license is of the same quantity as BASE CPS License. This license supports 5 CPS capacity to the PSX server.	Node Locked
POL-SWE-SIPSCP-100CPS ²	This license provides SIP SCP functionality on Ribbon PSX Policy Server. For egress SIP SCP traffic, the license is of the same quantity as BASE CPS License. This license supports 100 CPS capacity to the PSX server.	Node Locked
POL-SWE-SIPSCP-5CPS ²	This license provides SIP SCP functionality on Ribbon PSX Policy Server. For egress SIP SCP traffic, the license is of the same quantity as BASE CPS License. This license supports 5 CPS capacity to the PSX server.	Node Locked
POL-SWE-TCAP-100CPS ²	This license provides ANSI TCAP functionality on Ribbon PSX Policy Server. For egress ANSI TCAP traffic, the license is of the same quantity as BASE CPS License. This license supports 100 CPS capacity to the PSX server.	Node Locked
POL-SWE-TCAP-5CPS ²	This license provides ANSI TCAP functionality on Ribbon PSX Policy Server. For egress ANSI TCAP traffic, the license is of the same quantity as BASE CPS License. This license supports 5 CPS capacity to the PSX server.	Node Locked
POL-SWE-AINVPN-100CPS	This license provides AIN Voice VPN functionality on Ribbon PSX Policy Server. For egress AIN Voice VPN traffic, the license is of the same quantity as BASE CPS License. This require the same quantity of POL-TCAP-100CPS licenses.	Node Locked

License	Description	Displayed on RAMP
POL-SWE-AINVPN-5CPS ²	This license provides AIN Voice VPN functionality on Ribbon PSX Policy Server. For egress AIN Voice VPN traffic, the license is of the same quantity as BASE CPS License. This requires the same quantity of POL-TCAP-5CPS licenses.	Node Locked
POL-SWE-GSM-100CPS ²	This license provides GSM functionality on Ribbon PSX Policy Server. For egress GSM traffic, the license is of the same quantity as BASE CPS License. This requires the same quantity of POL-ITUTCAP-100CPS license.	Node Locked
POL-SWE-GSM-5CPS ²	This license provides GSM functionality on Ribbon PSX Policy Server. For egress GSM traffic, the license is of the same quantity as BASE CPS License. This requires the same quantity of POL-ITUTCAP-5CPS license.	Node Locked
POL-SWE-IS41-100CPS ²	This license provides IS-41 functionality on Ribbon PSX Policy Server. For egress IS-41 traffic, the license is of the same quantity as BASE CPS License. This requires the same quantity of POL-TCAP-100CPS licenses.	Node Locked
POL-SWE-IS41-5CPS ²	This license provides IS-41 functionality on Ribbon PSX Policy Server. For egress IS-41 traffic, the license is of the same quantity as BASE CPS License. This requires the same quantity of POL-TCAP-5CPS licenses.	Node Locked
POL-SWE-LNP-100CPS ²	This license provides AIN LNP functionality on Ribbon PSX Policy Server. For egress AIN LNP traffic, the license is of the same quantity as BASE CPS License. This requires the same quantity of POL-TCAP-100CPS licenses.	Node Locked
POL-SWE-LNP-5CPS ²	This license provides AIN LNP functionality on Ribbon PSX Policy Server. For egress AIN LNP traffic, the license is of the same quantity as BASE CPS License. This requires the same quantity of POL-TCAP-5CPS licenses.	Node Locked
POL-SWE-TF-100CPS ²	This license provides AIN Toll Free functionality on Ribbon PSX Policy Server. For egress AIN Toll Free traffic, the license is of the same quantity as BASE CPS License. This requires the same quantity of POL-TCAP-100CPS licenses.	Node Locked

License	Description	Displayed on RAMP
POL-SWE-TF-5CPS ²	This license provides AIN Toll Free functionality on Ribbon PSX Policy Server. For egress AIN Toll Free traffic, the license is of the same quantity as BASE CPS License. This requires the same quantity of POL-TCAP-5CPS licenses.	Node Locked
POL-SWE-TRANS-100CPS ²	This license provides Number Translation functionality on Ribbon PSX Policy Server. For egress Number Translation traffic, the license is of the same quantity as BASE CPS License. This license supports 100 CPS capacity to the PSX server.	Node Locked
POL-SWE-TRANS-5CPS ²	This license provides Number Translation functionality on Ribbon PSX Policy Server. For egress Number Translation traffic, the license is of the same quantity as BASE CPS License. This license supports 5 CPS capacity to the PSX server.	Node Locked
POL-SWE-INAP-100CPS ²	This license provides the Intelligent Network Application Part (INAP) services. This allows for VoIP networks to access INAP SCPs for INAP-based services. This license supports 100 CPS capacity to the PSX server.	Node Locked
POL-SWE-INAP-5CPS ²	This license provides the Intelligent Network Application Part (INAP) services. This allows for VoIP networks to access INAP SCPs for INAP-based services. This license supports 5 CPS capacity to the PSX server.	Node Locked
POL-SWE-LNP-STORE-5CPS	This license provides Hosted Carrier ENUM service on the PSX (SWe). The license is of the same quantity as BASE 5 CPS license.	Node Locked
POL-SWE-LNP-STORE-100CPS	This license provides Hosted Carrier ENUM service on the PSX (SWe). The license is of the same quantity as BASE 100 CPS license.	Node Locked
POL-SWE-LCR-5CPS	This license provides PSX (SWe) to make routing decisions based on least-cost routing data and on QoS data. If this license is unavailable VBR data cannot be used in call processing. The license is of the same or lesser quantity as BASE 5 CPS license.	Node Locked

License	Description	Displayed on RAMP
POL-SWE- LCR-100CPS	This license provides PSX (SWe) to make routing decisions based on least-cost routing data and on QoS data. If this license is unavailable VBR data cannot be used in call processing. The license is of the same or lesser quantity as BASE 100 CPS license.	Node Locked

Note

- The licenses with superscript¹ indicate that the licenses are sold at the CPS rate and enforced at the CPS rate.
- The licenses with Superscript² indicate that the licenses are sold at CPS rate, but enforced as Feature ON/OFF license.

Note

- RAMP allows the association of the PSX SWe license feature only to PSX SWe nodes.
- The existing CPS license features cannot be associated with PSX SWe nodes.
- When registering a replica PSX using the node registration service, the replica PSX will initially have no CPS licenses associated with it. You need to manually associate licenses with the replica PSXs once they are registered with EMS.
- When a replica PSX node is unregistered, the associated licenses are retained. The associated licenses to the node are cleared only when the node is purged.

SBC Core (5x10, 5400, 7000, and SWe)

The RAMP only supports SBC licensing for the Network-Wide Domain Licensing (NWDL) mode. For the SBC licenses supported for NWDL, refer to [NWDL Feature License Keys](#).

Note

Node-Locked or NWL SBC licenses are installed directly into the SBC. For information on adding licenses directly to the SBC, refer to [System Administration - License Management](#).

MRFP Licenses

The RAMP supports MRFP licensing only for the Network-Wide Domain Licensing (NWDL) mode. Node-Locked or NWL licenses are installed directly into the MRFP.

DSI Licenses

The licenses are generated using the Node Locked License key. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#). These licenses are listed on the RAMP as Node Locked.

The following table summarizes the list of hardware based DSI feature licenses. All DSI licenses are based on the number of subscribers and are issued on a per CPU basis.

DSI-HW Feature Licenses

License (Feature ID)	Description
DSI-L0	The L0 license includes the following always available features: • All NFS Server features in support of GSX. • Traditional NFS-mode GSX event logging and CAM reception. • Optional streaming-mode GSX event logging and BCAM reception including optional CAM field selection/de-selection. • Housekeeping services for administrative management. • Transporter services for one-way transfer of CAM/BCAM files limited to a remote DSI-L1/L2 server.
DSI-L1	L1 license includes all L0 features and: • FileServices workflow functions for renaming, compression, and checksum of CAM files. • Transporter services for bi-directional data exchange with other network elements or Third Party servers.
DSI-L2	The L2 license includes all L1 features with the constraint that FileServices is limited to operational use on a single-node L2. In addition, the L2 license enables primary mediation capabilities and is the entry level for DSI translation services. Operations with custom adaptors requires this license at a minimum.
DSI-CL	The CL license enables cluster configurations that provide high availability (HA) and scalability. The CL license can be used in combination with other licenses: L2, AMA, SRS, BCAM-CONV. CL requires a minimum of two (2) nodes with a supporting RAID server. CL supports up to 16 nodes, two of which are directly attached to the RAID server.
DSI-AMA	The AMA license enables the Automatic Message Accounting (AMA) feature of DSI, which includes the generic AMA adaptors and the AMADNS interface to a DPMS. AMA requires license L2 as a prerequisite and is frequently used in combination with license CL.
DSI-BCAM-CONV	BCAM-CONV license enables GSX BCAM data to be re-formatted into legacy ASCII format. Any de-selected BCAM fields appear as null fields in the legacy ASCII format (with contiguous commas). The BCAM-CONV license may be used with any operating license L0, L1, or L2.
DSI-BROADCAST	The BROADCAST license enables the single source file transfer to multiple targets.

DSI Licenses

License (Feature ID)	Description	Displayed on RAMP
DSISWL0	This license provides Level 0 functionality on Ribbon DataStream Integrator.	Node Locked
DSISWL1	This license provides Level 1 functionality on Ribbon DataStream Integrator.	Node Locked
DSISWL2	This license provides Level 2 functionality on Ribbon DataStream Integrator.	Node Locked
DSISWCL	This license provides Clustering functionality on Ribbon DataStream Integrator.	Node Locked
DSISWAMA	This license provides AMA functionality on Ribbon DataStream Integrator. This license also requires the DSI node have a DSISWL2 license.	Node Locked
DSISWSRS	This license provides Subscriber Reporting Server functionality on Ribbon DataStream Integrator. This license also requires the DSI node have a DSISWL2 license.	Node Locked
DSISWADVCO RR	This license provides enhanced Correlation functionality on Ribbon DataStream Integrator. This license also requires the DSI node have a DSISWL2 license.	Node Locked
DSISWBCCAMC ONV	This license provides for DSI functionality allowing the translation of GSX binary stream to legacy ASCII format.	Node Locked
DSISWVRS	This license provides SMARRT VPN Reporting Server functionality on Ribbon DataStream Integrator. This license can be enabled only on DSI nodes licensed with DSISWL2 for Level 2 functionality.	Node Locked
DSISWSAI	This license provides Signaling Analysis Interface functionality on Ribbon DataStream Integrator. This license can be enabled only on DSI nodes licensed with DSISWL2 for Level 2 functionality.	Node Locked
DSISWBROAD CAST	This license allows the DSI Transporter Client and Remote Client to specify any number of target destinations for a single source.	Node Locked

DSI SWe

The RAMP License Manager lists all the available and registered DSI SWe nodes as targets for DSI SWe licenses. Feature ID for DSI virtual nodes is "SWe" instead of "SW" (non-virtual). DSI SWe license file attributes except for feature IDs. For example: ExpiryDate, lineId, and usageLimit, remain the same.

DSI SWe license feature IDs are associated only to DSI SWe nodes; DSI server nodes cannot be associated. You are allowed to associate and dissociate DSI SWe licenses. The DSI node is registered with EMS as a new sub-type to identify whether the node is registered as DSI or DSI SWe. EMS displays the DSI sub-type (SWe) in the node registration page for the DSI SWe nodes.

Alarms on Server based DSI licensing feature are also supported on DSI SWe. The license management and integrity requirements are the same for DSI SWe and server-based DSI.

You are allowed to install the license bundle with SWe features through the License Manager GUI. The SWe-based license is applicable for the DSI node running on a virtual box. When the user selects a SWe-based license feature, only the virtual DSI nodes and SWe nodes are listed for the selected node type. For non-SWe feature licenses, only non-virtual DSI servers are listed. Similarly, for association and dissociation, only the relevant licenses are listed for the selected node type.

DSI SWe Licenses

License (Feature ID)	Description	Displayed on RAMP
DSISWE-L0	This license provides Level 0 functionality on Ribbon Data Stream Integrator Virtual Machine.	Node Locked
DSISWE-L1	This license provides Level 1 functionality on Ribbon Data Stream Integrator Virtual Machine.	Node Locked
DSISWE-L2	This license provides Level 2 functionality on Ribbon Data Stream Integrator Virtual Machine.	Node Locked
DSISWE-AMA	This license provides AMA functionality on Ribbon Data Stream Integrator Virtual Machine. This license also requires the DSI Virtual Machine to have a DSISWE-L2 license.	Node Locked
DSISWE-BCAM-CONV	This license provides DSI functionality allowing the translation of GSX binary stream to legacy ASCII format.	Node Locked
DSISWE-SRS	This license provides Subscriber Reporting Server functionality on Ribbon Data Stream Integrator Virtual Machine. This license also requires the DSI Virtual Machine to have a DSISWE-L2 license.	Node Locked
DSISWE-SAI	This license provides Signaling Analysis Interface functionality on Ribbon Data Stream Integrator. This license can be enabled only on DSI nodes licensed with DSISWE-L2 for Level 2 functionality.	Node Locked

License (Feature ID)	Description	Displayed on RAMP
DSISWE-CL	This license provides Clustering functionality on Ribbon Data Stream Integrator Virtual Machine.	Node Locked
DSISWE-VRS	This license provides SMARRT VPN Reporting Server functionality on Ribbon Data Stream Integrator. This license can be enabled only on DSI nodes licensed with DSISWE-L2 for Level 2 functionality.	Node Locked
DSISWE-BROADCAST	This license allows the DSI Transporter Client and Remote Client to specify any number of target destinations for a single source.	Node Locked

SGX4000

The licenses are generated using the Node Locked License key. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#). These licenses are listed on the RAMP as Node Locked.

SGX4000 Licenses

License (Feature ID)	Description	Displayed on RAMP
SGX-SS7	This license authorizes TDM based SS7 capability on Ribbon SGX4000.	Node Locked
SGX-SIG	This license authorizes external SIGTRAN capability on Ribbon SGX4000.	Node Locked
SGX-CAP-SM	This license authorizes call processing (small capacity) capability on Ribbon SGX4000.	Node Locked
SGX-CAP-SM-TO-MED	This license authorizes call processing (medium capacity)) capability on Ribbon SGX4000.	Node Locked
SGX-CAP-MED-TO-LRG	This license authorizes call processing (large capacity) capability on Ribbon SGX4000.	Node Locked
SGX-DUAL-CE	This license authorizes dual CE redundancy capability on Ribbon SGX4000.	Node Locked
SGX-GR	This license supports Geographic Redundancy. It provides additional protection for the Application Servers against outages in the SS7 network.	Node Locked

License (Feature ID)	Description	Displayed on RAMP
SGX-SIG	This license authorizes external SIGTRAN capability on Ribbon SGX4000.	Node Locked
SGX-16NODES	This license enables the support of 16 nodes on Ribbon SGX4000.	Node Locked
SGX-32NODES	This license enables the support of 32 nodes on Ribbon SGX4000.	Node Locked

Note

The expiry date for SGX-16NODES and SGX-32NODES must be the same.

SGX4000 SWe

These licenses are generated using the Node Locked License key. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#). These licenses are listed on the RAMP as Node Locked.

SGX4000 SWe License

License (Feature ID)	Description	Displayed on RAMP
SGX-VIRTUAL	This license enables the SGX SWe on KVM.	Node Locked

Domain Locked Licenses on RAMP

In this section:

- [Domain Locked Licenses for PSX](#)
- [Domain Locked Licenses for SBC](#)
- [Domain Locked Licenses for SBC SWe Edge](#)
- [Domain Locked Licenses for MRFP](#)
- [Domain Locked Licenses for SLB](#)

The SBC Core Portfolio (SBC 5400, SBC 7000, SBC SWe, and SBC CNe) and PSX deployments support a domain locked licensing model (DL). In contrast to the node locked licensing, a domain locked license is tied to an administrative domain rather than the hardware ID for a specific host server or the UUID for a particular node instance. A domain locked license is bound to the domain through public/private key-pairing and it defines the

features and capacity allowed for all the nodes within the domain. Domain locked licenses provide flexibility in cloud environments where the number and placement of nodes vary sometimes.

The domain locked licenses are implemented using license management capabilities within the Ribbon Application Management Platform (RAMP). RAMP provides the public key used to bind the license to the local domain and is used for associating license data with eligible nodes.

This section lists Domain Locked Licenses on the RAMP. These licenses are generated using the Domain Locked License key. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#). These licenses are listed on the RAMP as Domain Locked.

Domain Locked Licenses for PSX

DL licenses are generated using the Domain Locked License key and are displayed as "Domain Locked" on RAMP. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#).

License ID	Description
POL-TESTDB-D	Enables Test Database functionality.
POL-VPN-D	Enables Voice VPN Business Group functionality.
POL-SPE-D	Enables Service Profile Editor based scripting fun.
POL-GLOBAL-D	Disables CPS based enforcement.
POL-BASESW-D	Base Routing. Mandatory license on call processing.
POL-SIP-D	SIP Proxy and Re-director to support third party.
POL-ENUMSVR-D	Enables the PSX to act as an ENUM Server for third.
POL-ENUMCLT-D	Enables ENUM lookups to external SCPs.
POL-IN-D	Enables IN capability for CNAM lookups.
POL-ITUTCAP-D	Enables ITUTCAP Protocol.
POL-SIPSCP-D	Enables SIP based SCP lookups.
POL-TCAP-D	Enables ANSI TCAP Protocol.
POL-GLNP-D	Enables LNP lookup capability for non-North America.
POL-GSM-D	Enables MAP protocol lookups to HLR.
POL-IS41-D	Enables IS41 protocol based lookups.

License ID	Description
POL-LNP-D	Enables LNP lookup capability for North America.
POL-TF-D	Enables TollFree lookup capability.
POL-TRANS-D	Enables on-board number translations.
POL-H323PGK-D	Enables H.323 Gatekeeper functionality.
POL-LCR-D	Enables Least Cost Routing functionality.
POL-OBRDLNP-D	Enables on-board number portability.
POL-STSH-D	Enables STIR/SHAKEN feature.
POL-RCD-D	Enables Rich Call Data feature.
POL-REST-INST-D	Enables Instance Based License for Generic Routing. Note The equivalent Node Locked License ID is POL-SWE-RESTINST-ENF (1 quantity each similar to SPE)

For more information, refer to the PSX document [Domain Locked Licensing](#).

Domain Locked Licenses for SBC

These licenses are generated using the Domain Locked License key. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#).

Feature ID	Usage	Display on RAMP
DSP-AMDisplaRNB-D	RTU media interworking using AMRNB. Use license to enable AMR-NB audio transcoding.	Domain Locked
DSP-AMRWB-D	RTU media interworking using G.722.2/AMR-WB. Use this license to enable AMR-WB audio transcoding.	Domain Locked

Feature ID	Usage	Displa yed on RAMP
DSP-EVRC-D	RTU media interworking using EVRC. Use this license to enable all variants of EVRC audio transcoding. Note: This license is not applicable to SBC SWe because EVRC is not supported.	Doma in Locke d
DSP-EVS-D	RTU media interworking using EVS. Use this license to enable all variants of EVS transcoding.	Doma in Locke d
DSP-L16-D	Enables LINEAR16 (Linear PCM) codec processing on any RTP media session receiving Virtual DSP services (latter activated with the VDSP-RTU-D).	Doma in Locke d
DSP-OPUS-D	This adds OPUS codec processing to any RTP media session receiving Virtual DSP services (the latter is activated with the VDSP-RTU-D).	Doma in Locke d
DSP-SILK-D	RTU media interworking using SILK. Use license to enable SILK transcoding.	Doma in Locke d
ENCRYPT-D	Encryption function for signaling using TLS, IPsec.	Doma in Locke d
LB- INSTANCE-D	Activates an SBC SWe SLB (SIP-Aware Front-End Load Balancer) instance within the domain for operation. SIP sessions carried across the SLB are licensed separately (SBC-LB-D).	Doma in Locke d
SBC-1X10GMP-D	SBC 5400 RTU license to enable media port(s) operating at 10 Gbps. This will activate two 10 Gbps packet ports.	Doma in Locke d
SBC-4X1GMP-D	SBC 5400 RTU license to enable all four media ports. each operating at 1 Gbps.	Doma in Locke d

Feature ID	Usage	Displa yed on RAMP
SBC-CNE- INSTANCE-D	This license differentiates the CNF deployments from those handled by the same RAMP. Without this license, total calls up to 47 concurrent calls are supported on a CNe deployment. The maximum active SC pods can be 47, one call per SC pod is supported. The OAM is the only pod which will connect to the license manager. In case of completion of 90 days grace period, OAM communicates the information to SC pod to stop processing the calls.	Doma in Locke d
SBC-ETSI-LI- D	Enables ETSI/3gpp-related Lawful Intercept services.	Doma in Locke d
SBC-FIPS- INST-D	Enables SBC device-wide FIPS-140 supporting operation.	Doma in Locke d
SBC-FIPS- RTU-D	Enables SIP session-specific FIPS-140 supporting operation.	Doma in Locke d
SBC-LB-D	Activates support for a SIP session on an SBC SWe SLB (SIP-Aware Front-End Load Balancer) instance. The SLB instance is licensed separately (LB-INSTANCE-D).	Doma in Locke d
SBC-LI-D	Enables PacketCable-related Lawful Intercept services.	Doma in Locke d
SBC-MRF- RTU-D	This license is required to enable transcoding using an external Media Resource Function (MRF) device. The SBC-MRF-RTU-D license is not a substitute for the SBC-RTU-D session license. Both licenses are required to allow a session towards the MRF. The SBC-MRF-RTU-D license is only applicable to the S-SBC when deploying the distributed-SBC architecture.	Doma in Locke d
SBC-POL- E911-D	RTU license for E911 service.	Doma in Locke d

Feature ID	Usage	Displa yed on RAMP
SBC-POL-ENUM-D	SBC ERE support for accessing ENUM databases.	Doma in Locke d
SBC-POL-RTU-D	Enables on-board Advanced ERE (Embedded Routing Engine) services query support for a given SIP session (The latter is activated with the SBC-RTU-D license).	Doma in Locke d
SBC-PSX-RTU-D	Enables off-board PSX policy and routing services query support for a given SIP session (latter activated with the SBC-RTU-D).	Doma in Locke d
SBC-RCS-D	Enables OOD (Out of Dialog) SIP session-related RCS (Rich Communications Services) support.	Doma in Locke d
SBC-RTU-D	Controls the right-to-use (RTU) for SIP sessions. The following types of media sessions are enabled: • Pass-through audio (no DSPs) • Pass-through audio and video (no conferencing) • Transcoded audio	Doma in Locke d
SBC-SIP-I-D	SIP-I interworking function.	Doma in Locke d
SBC-SIP323-D	SIP/H.323 Interworking function.	Doma in Locke d
SBC-SIPREC-D	SIPREC session recording support.	Doma in Locke d
SBC-STSH-D	Adds STIR SHAKEN-related processing on an SIP session (latter activated with the SBC-RTU-D).	Doma in Locke d

Feature ID	Usage	Displa yed on RAMP
SBC-SURV-D	Adds Local Survivability support on an SIP session (latter activated with the SBC-RTU-D).	Doma in Locke d
SBC-TOIP-D	Enables T.140/Text over IP processing on any RTP media session receiving Virtual DSP services (latter activated with the VDSP-RTU-D).	Doma in Locke d
SBC-VIDEO-D	Video interworking support, including Content Sharing (BFCP), Far-End Camera Control (FECC) and H.239 for H.323.	Doma in Locke d
SIP-REG-D	DL Feature license for SIP Registrar functionality (Domain E-LIC FOR SIP-REG ON SBC Core). For DL licenses, the maximum license count is equal to the maximum registrations supported by the SBC.	Doma in Locke d
SRTP-D	Encryption function for media using Secure Real-time Transport Protocol (SRTP).	Doma in Locke d
SWE- INSTANCE-D	Activates an SBC SWe instance within the domain for operation.	Doma in Locke d
VDSP-RTU-D	Enables RTP media processing services in the SBC Core software based products (SBC SWe, SBC CNe).	Doma in Locke d
WEBSOCKET -D	Enables WebRTC-related processing on an SIP session (latter activated with the SBC-RTU-D).	Doma in Locke d

For more information, refer to [Domain Locked Licensing Feature License Keys](#).

Domain Locked Licenses for SBC SWe Edge

These licenses are generated using the Domain Locked License key. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#).

Feature ID	Usage	Displayed on RAMP
SRTP-D	Encryption (RTP ↔ SRTP) in a single SIP session's RTP media stream.	Domain Locked
ENCRYPT-D	Encryption (TLS) in a single SIP session's signaling (TCP) connection.	Domain Locked
SBC-SWE-EDGE-SA-INSTANCE-D	Standalone (non-High Availability) SBC SWe Edge instance licensed for use in the customer's NWDL domain.	Domain Locked
SBC-EDGE-SA-HIGH-D	Standalone (non-High Availability) SBC SWe Edge instance licensed to carry in excess of 100 simultaneous SIP sessions.	Domain Locked
DSP-AMRNB-D	AMR Narrowband for a single SIP Session.	Domain Locked
SBC-SA-RTU-D	Single basic SIP session with RTP media licensed for use in any Standalone (non-High Availability) SBC.	Domain Locked
SIP-REG-D	250 SIP Registrants successfully registering to the SBC's SIP Registrar.	Domain Locked
SBC-SIPREC-D	SIPREC call recording support for a single SIP session.	Domain Locked
VDSP-SA-RTU-D	Transcode support for a single SIP session's media stream in a Standalone (non-High Availability) SBC.	Domain Locked

Feature ID	Usage	Displayed on RAMP
TEAMS-SBA-D	Direct Routing SBA in the low capacity (under 1000 sessions) SBC Edge device.	Domain Locked
DSP-AMRWB-D	AMR Wideband support in a single SIP session.	Domain Locked
DSP-SILK-D	SILK codec support in a single SIP session.	Domain Locked
SBC-VIDEO-D	Video-related RTP media support in a single SIP session.	Domain Locked
SBC-SWE-EDGE-INSTANCE-D	Standalone (non-High Availability) SBC SWe Edge instance licensed for use in the customer's NWDL domain.	Domain Locked

Domain Locked Licenses for MRFP

These licenses are generated using the Domain Locked License key. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#).

Feature ID	Usage	Displayed on RAMP
MRFP-SWE-BASE-D	Network wide domain-locked MRFP SWe based system, which includes OS. No sessions, and sold in blocks of 1.	Domain Locked
MRFP-BASE-SW-HA-5	MRFP base software, 5+1 HA. Sold in blocks of 6.	Domain Locked

Feature ID	Usage	Displayed on RAMP
MRFP-SWE-TXN1-D	Network wide domain-locked transcode license for MRFP SWe. 1-2500 sessions, sold in blocks of 250.	Domain Locked
MRFP-SWE-TXN1-HA-D	Network wide domain-locked transcode license for HA SWe. 1-2500 sessions, sold in blocks of 250.	Domain Locked
MRFP-SWE-TXN2-D	Network wide domain-locked transcode license for MRFP SWe. 2501-5000 sessions, sold in blocks of 250.	Domain Locked
MRFP-SWE-TXN2-HA-D	Network wide domain-locked transcode license for HA SWe. 2501-5000 sessions, sold in blocks of 250.	Domain Locked
MRFP-SWE-TXN3-D	Network wide domain-locked transcode license for MRFP SWe. 5001-10,000 sessions, sold in blocks of 250.	Domain Locked
MRFP-SWE-TXN3-HA-D	Network wide domain-locked transcode license for HA SWe. 5001-10,000 sessions, sold in blocks of 250.	Domain Locked
MRFP-SWE-TXN4-D	Network wide domain-locked transcode license for MRFP SWe. 10,001-20,000 sessions, sold in blocks of 250.	Domain Locked
MRFP-SWE-TXN4-HA-D	Network wide domain-locked transcode license for HA SWe. 10,001-20,000 sessions, sold in blocks of 250.	Domain Locked
MRFP-SWE-TXN5-D	Network wide domain-locked transcode license for MRFP SWe. 20,001-50,000 sessions, sold in blocks of 250.	Domain Locked

Feature ID	Usage	Displayed on RAMP
MRFP-SWE-TXN5-HA-D	Network wide domain-locked transcode license for HA SWe. 20,001-50,000 sessions, sold in blocks of 250.	Domain Locked
MRFP-SWE-TXN6-D	Network wide domain-locked transcode license for MRFP SWe. 50,001+ sessions, sold in blocks of 250.	Domain Locked
MRFP-SWE-TXN6-HA-D	Network wide domain-locked transcode license for HA SWe. 50,001+ sessions, sold in blocks of 250.	Domain Locked
MRFP-SWE-NBGSM-D	Network wide domain-locked codec license for AMR-NB use on core MRFP. Sessions sold in blocks of 250.	Domain Locked
MRFP-SWE-WBGSM-D	Network wide domain-locked codec license for AMR-WB use on core MRFP. Sessions sold in blocks of 250.	Domain Locked
MRFP-SWE-CDMA-D	Network wide domain-locked codec license for EVRC use on core MRFP. Sessions sold in blocks of 250.	Domain Locked
MRFP-SWE-EVS-D	Network wide domain-locked codec license for EVS use on core MRFP. Sessions sold in blocks of 250.	Domain Locked
MRFP-GPU-NVIDIA-V100	MRFP NVIDIA V100 GPU transcoding license. Sold in blocks of 1.	Domain Locked
MRFP-CAPACITY	Domain wide capacity license for MRFP. Sold in blocks of 1.	Domain Locked

For more information, refer to [MRFP Licensing](#).

Domain Locked Licenses for SLB

These licenses are generated using the Domain Locked License key. To obtain the license key, refer to [Find License Keys for Obtaining Licenses](#).

Feature ID	Usage	Displayed on RAMP
LB-INSTANCE-D	The Domain Locked license to run the SLB.	Domain Locked

Performance Management

In this section:

- [Planning for Performance Management](#)
- [Define Which Statistics to Collect](#)
- [Define Which Statistics to Export](#)
- [Specify How Long to Retain Statistics Data](#)
- [Enable Statistics Collection and Exporting](#)
- [Generate PM Reports and Report Templates](#)
- [Define Statistics Values that Trigger Alarms](#)

Related articles:

- [Performance Management Workflows](#)
- [Collect and Export Device Statistics](#)
- [Working with Reports](#)
- [Define Performance Thresholds](#)
- [Exported Statistics](#)

The Ribbon Application Management Platform (RAMP) Performance Management (PM) service regularly collects statistics from managed devices so that enterprises can use the data to monitor the health, operational efficiency, and usage levels of their devices. The PM service provides both a flexible reporting framework for working with these statistics within RAMP and an exporting function for sending selected statistics to external systems using SFTP. For deployments that are licensed to use a post-paid billing model, PM statistics collection is an essential component in reporting usage levels to Ribbon.

The following sections introduce the key concepts and capabilities of RAMP performance management.

Planning for Performance Management

Each type of device generates a variety of statistics that the RAMP PM service can collect. Enterprises must evaluate the statistics options to determine which ones provide relevant information for monitoring their network by taking into consideration their specific network components and call traffic patterns. The RAMP administrator can then tailor their system to collect useful data and avoid processing statistics that provide minimal value. Administrators can similarly tailor their choices of statistics to export to ensure that only relevant statistics are

forwarded to an external system, such as an Operations Support System (OSS). Careful selection of collection and export criteria also assists with planning for data retention by reducing the storage requirements.

Refer to [Exported Statistics](#) for information on the statistics categories and metrics to plan which statistics to collect and export.

For businesses that want to implement a PM “operator” role that limits some users to working with PM reports only, RAMP administrators must ensure that they configure RAMP resource groups and user groups appropriately. Resource groups logically group devices within the network and user groups determine which users can work with particular resource groups. Operators can only access reports for devices to which they have access. Therefore, administrators must be sure PM operators are members of user groups with access to the devices for which they will run reports.

Refer to [Work with Resource Groups](#) for more information on resource groups.

Refer to [Add User Groups](#) for more information on creating user groups.

Define Which Statistics to Collect

When a device registers, either manually or dynamically, RAMP automatically assigns it a default PM collection profile based on its device type. A device’s collection profile specifies which statistics are generated on that device and which are collected by RAMP. The default profiles specify to generate and collect all types of statistics available from the device. For some types of devices, such as the Ribbon SBC or PSX, the potential list of statistics is quite extensive. Therefore, in many cases the collection criteria should be modified to disable generating and collecting unneeded statistics to reduce processing overhead and storage requirements. RAMP administrators can create one or more customized collection profiles based on their network characteristics and assign them to their devices rather than the default profile. The same profile can be assigned to multiple devices, as appropriate.

Refer to [Define Statistics to Collect](#) for more information on PM collection profiles.

Define Which Statistics to Export

Similar to collection profiles, RAMP automatically assigns a default PM export profile when a device registers, based on its device type. An export profile specifies which statistics to export, the destination, and how often to export the statistics. The default profiles specify to export all categories of statistics to a local location at a high (5-minute) frequency. As with the default collection criteria, the default export settings may be too broad for many networks and can result in more export data than is really needed. RAMP administrators can create one or more customized export profiles that select the optimal statistics to export, specify the export destination, and select the frequency of export. An export profile can specify more than one destination location for the statistics data if needed and the same profile can be assigned to multiple devices, as appropriate.

Refer to [Define Statistics to Export](#) for more information on PM export profiles.

Specify How Long to Retain Statistics Data

Depending on the number and type of nodes in a network, PM data can require a significant amount of storage space. Each enterprise must develop a data retention policy that fits their network characteristics and resources. RAMP allows the administrator to specify how long to retain each type of statistic individually, with an initial default of one week for interval data, and four weeks for both daily and hourly aggregate data.

Refer to [Define Data Retention Periods](#) for more information on configuring data retention.

Enable Statistics Collection and Exporting

Although RAMP assigns default collection and export profiles to each registered device automatically, the administrator must ensure that collection and export are enabled on each device. This provides the administrator an opportunity to adjust the collection and export criteria before activating those processes. However, if RAMP is

licensed to support post-paid billing, RAMP automatically enables PM statistics collection to ensure that license-related usage statistics can be regularly reported to Ribbon. Note that to enable post-paid billing, RAMP must be licensed to collect PM-based licensing statistics (RAMP_LIC_AUDIT_REPORT license key) and to generate usage reports (RAMP_LIC_MANUAL_REPORT or RAMP_LIC_AUTO_REPORT license keys).

Refer to [Assign Collection and Export Profiles](#) for information on enabling PM collection and exporting.

Refer to [Set Up Reporting for Post-Paid Billing](#) for more information on post-paid billing.

Generate PM Reports and Report Templates

To aid in monitoring network devices, an operator can run a PM report to retrieve a set of statistics data from a specified device, for a specific date range, and with a selected level of data granularity. RAMP returns these statistics in both tabular and graphical form so the operator can evaluate the data. Depending on the type of statistic involved, the operator might also provide additional criteria such as a port number, trunk group, or another index value that further refines the report data. Users also have the option to download their reports in either CSV or PDF format.

Operators or administrators must create report templates for each type of report they want to run. A report template specifies a type of device, a statistics group, and which individual metrics within that group (up to 10) to include in the report. Operators select from the configured report templates to run their individual reports.

Refer to [Working with Reports](#) for more information on reports and report templates.

Define Statistics Values that Trigger Alarms

To highlight when specific values occur within in the PM data, the RAMP administrator can create PM thresholds for specific metrics. Thresholds specify a triggering value for the selected PM metric. When that value is met or exceeded, it triggers an alarm within the RAMP fault management service with a severity level specified in the threshold configuration. For example, a threshold could be set to trigger a major alarm when a specified number of call failures occur within an interval, or a critical alarm when a specified CPU utilization percentage is reported. The threshold configuration also specifies a clearing value for the metric that triggers a clearing alarm once the clearing value is met.

Refer to [Define Performance Thresholds](#) for more information on PM thresholds.

Performance Management Workflows

The Ribbon Application Management Platform (RAMP) Performance Management (PM) service supports a range of PM tasks. The following workflows outline the main steps required to complete key PM tasks. Each step links to a page to obtain detailed information and procedures.

- [Profile Assignment](#) – configure performance data collection and export.
- [Creating and Running Reports](#) – create reports from performance metrics.
- [Configuring Threshold Alarms](#) – define performance metric thresholds that trigger alarms.
- [Configuring Data Retention](#) – specify how long RAMP retains performance data.

Prerequisite

For all PM workflows, devices must be registered with RAMP to enable the collection and forwarding of performance metrics.

Workflow – Profile Assignment

Step	Action
1	Verify and customize the Collection Profile for each managed device if required
2	Verify and customize the Export Profile for each managed device
3	Assign/Enable the Collection Profile and Export Profile

Workflow – Creating and Running Reports

Step	Action
1	Create report templates to specify which statistics to include in a report
2	Create reports to specify and save a set of runtime details
3	Run a report

Workflow – Configuring Threshold Alarms

Step	Action
1	Create alarm thresholds for specific performance metrics
2	Use fault management to monitor for threshold alarms

Workflow – Configuring Data Retention

Step	Action
1	Configure data retention intervals for specific types of statistics

Collect and Export Device Statistics

Related articles:

- [Define Statistics to Collect](#)
- [Define Statistics to Export](#)
- [Assign Collection and Export Profiles](#)
- [Define Data Retention Periods](#)

The Ribbon Application Management Platform (RAMP) allows you to monitor the performance of devices registered on it. The Performance Management service lets you configure what performance statistics to collect and also to set threshold values for performance measures. Instead of logging into each device to monitor its performance, with RAMP you can collect and analyze the performance metrics of a group of devices from a central console. Performance management profiles are created for this and performance statistics are collected periodically using protocols like SNMP and SFTP.

To monitor the performance of registered devices using the RAMP Performance Management service:

- Create collection profiles to decide which statistics to collect from which node.
- Define export parameters to decide which statistics to export and to what destination.
- Enable the required collection and export profiles.
- Define retention periods for performance statistics.

Define Statistics to Collect

In this section:

- [Modify a Collection Profile](#)
- [Delete a Collection Profile](#)

Related articles:

- [Configure Overrides for Statistics in Collection Profiles](#)
- [Configure Performance Management Collection Options](#)

On Ribbon Application Management Platform (RAMP), performance management data collection is managed using collection profiles. The collection profile defines which performance statistics to collect from a registered device and sets the collection frequency. This allows you to refine and customize data collection for individual or group nodes. Collection profiles are specific to the device type and interface used to collect data.

Default collection profiles are available for each interface type of every device registered on RAMP.

Every device registered on RAMP is assigned a collection profile by default. Since SFTP is the preferred interface for devices which support both SNMP and SFTP, default SFTP profiles are assigned to such devices by default.

Note

RAMP collects only active OAM statistics from the SBC CNe.

Create a Collection Profile

Use the following procedure to create a collection profile for a device.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Profile Management > Collection Profiles**.
3. Click **Add Profile**.
4. Enter a name for the collection profile.

Note

For GSX devices, the collection profile name should contain alphanumeric characters with a maximum length of 23 characters.

5. Select the type of node from the **Node Type** list.
6. Select the interface type to collect the data from the **Interface Type** list.
7. Select how frequently to generate a device statistics file from the **Statistics File Generation Frequency (on Device)** list. PSX Policy Servers and SBC Core nodes with SFTP interfaces generate statistics files. The RAMP PM service can directly collect these files from the devices. For every other device, RAMP performs in-memory queries to collect performance statistics.
8. Select the data/file collection frequency on the RAMP from the **Data/File Collection Frequency (on EMS)** list.
9. The **Statistics Table** is automatically populated with the statistics available for the node type and interface type you selected.
All statistics are enabled by default. Click to disable the **Collection** toggle adjacent to the statistics you do not want RAMP to collect.
You can enable or disable the statistics generation if statistics file generation is available for the selected node type. If you disable generation for a statistic, collection of that statistic is automatically disabled. The collection and generation of license usage statistics cannot be disabled in a collection profile. The collection toggles for these statistics show as enabled, but cannot be changed.
10. (Optional) You can reset the file generation and collection status to its default states (**Generation** and **Collection** in enabled states) by selecting the checkbox next to the statistic you want to reset and selecting **Reset to Defaults** from the **Select Action** menu.
11. Click **Save**.

Modify a Collection Profile

To edit an existing collection profile:

Start

1. Navigate to **Observability > Performance Management > Profile Management > Collection Profiles**.
2. In the collection profiles list, click on the collection profile to edit.
3. Make required changes to the collection profile settings.

Note

You cannot edit the **Node Type** and **Interface Type** once it is set while creating a collection profile.

4. Click **Save**.

Delete a Collection Profile

To delete an existing collection profile:

Start

1. Navigate to **Observability > Performance Management > Profile Management > Collection Profiles**.
2. Select **Delete** from the Action list for the collection profile you want to delete.
3. Confirm the deletion when prompted.

Configure Overrides for Statistics in Collection Profiles

The (Ribbon Application Management Platform) Performance Management (PM) service lets you configure overrides for individual performance statistics in a Collection Profile. With an override, you can enable or disable collection of a statistic or change the frequency at which it is collected.

Refer to [Define Statistics to Collect](#) for information on how to create a Collection Profile.

Prerequisites

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to Observability > Performance Management > Profile Management > Collection Profiles.
3. Select the Collection Profile for which you want to define overrides.
4. In the Statistic Table, select the checkbox next to one or more statistics for which you want to configure an override.
5. Select Override Selected from the Select Action menu. Configure the following information in the Override Statistic(s) for Collection window:

Field	Description
Collection	Enable or disable the collection of the selected statistic(s) using the Collection toggle.
Collection Frequency	Select the data/file collection frequency for the selected statistic(s).

6. Click Save to save the configuration changes.

Configure Performance Management Collection Options

In this section:

- [Configure Management Settings for Collection Profiles](#)
- [Configure Collector Process](#)
- [Configure Collection Scheduling Settings](#)
- [Configure SFTP Collector Settings](#)

The Ribbon Application Management Platform (RAMP) Performance Management (PM) service lets you configure administrative options that impact when it collects performance data and how it handles assigning collection profiles to devices. The PM service also enables you to specify data collection parameters for PM data collected using SFTP.

Use the procedures in this section to configure PM collection options.

Configure Management Settings for Collection Profiles

Configure the RAMP PM service administrative settings to improve the network efficiency. You can set a timeout interval for pushing collection profiles to a device and limit the maximum number of collection profiles created for

a device. You can also set the maximum number of times the RAMP tries to push the collection profile to a device and define the time delay between each try.

Prerequisite

You require Super User privileges for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Administration**.
3. In the **Profile Assignment Configuration** area under **Collection Profile Management**, configure the following options:

Field	Length/Range	Description
Timeout for profile enabling operation	1-240	Enter a timeout limit when the PM service assigns a collection profile to the device. After the timeout interval, the PM service stops trying to enable the collection profile on the device. The default value is "120".
Maximum profile per device per interface	5-10	Enter the maximum number of profiles created per device per interface type. The default value is "5".
Collection Profile Retry Count	1-3	Enter the number of times the RAMP should retry pushing a collection profile to a device. The default value is "1".
Delay Between Collection Profile Retries	1-30	Enter a time interval between each unsuccessful collection profile application retry. The default value is "5".

4. Click **Save**.

Configure Collector Process

Configure the PM stats collector to enable or disable running the JMX and SNMP collector processes. Disabling the JMX and SNMP PM stats processes for networks with devices supporting only SFTP-based collection ensures that the RAMP system resources are freed. The changes will take a few minutes to reflect in the backend.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Administration**.
3. In the **Collector Process Configuration** area under **Collector**, configure the following:

Field	Description
Disable JMX Collector	Enable this field to stop the JMX collector process. By default, this button is disabled.

Field	Description
Disable SNMP Collector	Enable this field to stop the SNMP collector process. By default, this button is disabled.

Configure Collection Scheduling Settings

Configure the RAMP PM service to manage collection scheduling settings, including adding offset periods at the start and end of a collection interval. The PM service waits for the specified start-offset period before starting statistics collection and stops the collection before the specified end-offset period.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Administration**.
3. In the **Collector Scheduling Configuration** area under **Collector**, configure the following options:

Field	Length/Range	Description
Randomize Poll Start Offset Secs	1-120 seconds.	Enter a duration, in seconds, to wait at the start of a polling interval before starting any polling to randomize collection across the interval. The default value is "45" seconds.
Randomize Poll End Offset Secs	1-180 seconds.	Enter a duration, in seconds, at the end of a polling interval to no longer start polling more devices when randomizing collection across the interval. The default value is "135".

4. Click **Save**.

Configure SFTP Collector Settings

Configure SFTP collector options. RAMP lets you specify whether to collect backlog files and how long to wait for an SFTP connection to open.

Prerequisites

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Administration**.
3. In the **SFTP Collector Configuration** area under **Collector**, configure the following options:

Field	Length/Range	Description
Collect backlog Files	NA	Select to enable RAMP to collect backlog files if there is an interruption in PM data collection. RAMP collects all files that are in NFS after application restart. By default, this is enabled.
Number of backlog files to fetch	1-12	Enter the number of backlog statistics files to collect from a device. This is the number of intervals over which backlog files are collected. The value range is between 1 (Previous Interval) and 12 (1 hour) per device. The default value is "1".
Secure FTP Poller Connection Timeout	1-120	Enter the interval, in seconds, that you want the secure FTP poller to wait before opening a secure FTP connection. the default value is "20".

4. Click **Save**.

Define Statistics to Export

In this section:

- [Configure Export Type](#)
- [Define Export Destinations](#)
 - [Add an Export Location](#)
 - [Modify an Export Location](#)
 - [Delete an Export Location](#)
- [Configure Export Profiles](#)
 - [Create an Export Profile](#)
 - [Modify an Export Profile](#)
 - [Delete an Export Profile](#)

Related articles:

- [Configure Overrides for Statistics in Export Profiles](#)
- [Configure Performance Management Export Options](#)
- [Reordering Exported PM CSV Files](#)
- [Backlog Collection of SBC, MRFP, and PSX Performance Management Data](#)

The Ribbon Application Management Platform (RAMP) Performance Management (PM) service lets you export selected performance data in CSV format to your specified location. The location can be on the local system or an external destination.

To export PM data, select an export type to define the file structure for the exported data and configure one or more export destinations. You must also configure one or more Export Profiles. In an Export Profile specify details about the export such as the statistics to export, how often to export, data granularity, and the destination location.

Use the following procedures to configure PM data export.

Configure Export Type

Select how you want to arrange PM data in the exported files.

Prerequisite

Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Profile Management > Export Profiles**.
3. Select an option from the **Export Type** list:
 - **Per Node Export**—The statistics data for each node is exported as a separate file.
 - **Per Profile Export**—The statistics data for all nodes assigned with the same profile is exported as a single file.
 - **All Nodes Export**—The statistics data for all nodes of a node type are exported as a single file.

Define Export Destinations

Configure the destinations to export the statistics files. The locations that you define here are available to include in an Export Profile.

Add an Export Location

Use the following procedures to add an export location:

Prerequisite

Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Profile Management > Export Profiles**.
3. Select the **Export Locations** tab.
4. Click **Add Location**.
5. Enter the following information:

Field	Description
Localhost	Select this checkbox if the destination is on the local system. If you specify a local system, you only need to provide a name and directory. The other options are not required.
Location Name	Enter a name for the location.
IP Address	Enter an IP address for the host system where the RAMP PM service sends the CSV files.
Directory	Enter the directory location on the host system where you want RAMP to place the exported CSV files. If the location is local, specify a subdirectory of <code><BASE_DIR>/weblogic/sonusEms/data/pm_archive</code> .

Field	Description
Use SSH Key	Select this checkbox if the <code>ssh</code> keys are already set. To use this option, you first save the <code>ssh</code> keys of RAMP to the external location, refer to Create a New Location to Save the SSH Key .
Username & Password	If the export location requires a username and password for access, enter these in the fields provided.

- Click **Save** to save the Export Location.

Modify an Export Location

To modify an export location:

- Navigate to **Observability > Performance Management > Profile Management > Export Profiles**.
- Select the **Export Locations** tab.
- In the export locations list, click on the export location to edit.
- Make required changes to the export location settings.
- Click **Save**.

Delete an Export Location

To delete an export location:

- Navigate to **Observability > Performance Management > Profile Management > Export Profiles**.
- Select the **Export Locations** tab.
- Click the **Delete** icon corresponding to the export location you want to delete.
- Confirm the deletion when prompted.

Configure Export Profiles

In RAMP, PM data export is managed using export profiles. Configure an export profile to define where you want to export the performance data, which performance statistics to export, and also to define the export frequency. You can also define the granularity of the export data.

RAMP provides a default export profile for each type of device and for all devices collectively. The PM service assigns a default export profile to each device based on the device type.

Create an Export Profile

Use the following procedures to create an export profile:

Prerequisite

Super User [privileges](#) for Performance Management.

Start

- Log on to the RAMP GUI.
- Navigate to **Observability > Performance Management > Profile Management > Export Profiles**.
- Select the **Export Profiles** tab.
- Click **Add Profile**.
- Enter a name for the export profile.
- Select how often the system performs exports of the performance data from the **Export Frequency** list. Ensure that **Export Frequency** is not less than **Collection Frequency**.

7. Select **Granularity** to define the contents (time slices) of the exported files. Select **All**, **1 hour** or **1 day**.
8. Select the **Export Aggregated Data** checkbox to export the aggregated performance statistics at the cluster level. You can export performance data as a single aggregated file for all nodes in a cluster. The following functions are used to aggregate the data over a cluster:

Function	Description
avg/average	Provides the average of all values in the cluster
sum	Provides the sum of all values in the cluster

Note

The directory structure for collecting statistics per-node level and per-cluster level is different. If you are collecting per-node level statistics and not using all node stats export, the per-node statistics are under directories with names of the nodes. If you are collecting per-cluster statistics (aggregated statistics), the aggregated- statistics in csv format are all put under directories with the names of the cluster. The directories for node names exists in directory structure at the same level as the cluster-directory name, when RAMP collects statistics at per-cluster level (aggregated statistics).

For example, if cluster-name is "sbc" and node names are "vsbc1" and "vsbc2" and statistics are aggregated at cluster-level, following is the directory structure. The aggregated cluster-level statistics are under cluster-name directory "sbc", while node-level statistics are under respective node-name directories ("vsbc1" and "vsbc2"):

sbc => csv files

vsbc1 => csv files

vsbc2 => csv files

9. Select the location to which to export data, from **Export Locations**.
10. Select one or more node types from the **Node Types** list.
11. The PM service automatically populates the **Statistics Table** with all types of PM statistics supported for the selected node type.
Enable or disable the export of these statistics using the **Export** toggle corresponding to that particular statistic.
12. (Optional) You can reset the export status to its default setting by selecting the checkbox next to the statistic you want to reset and selecting **Reset to Defaults** from the **Select Action** menu.
13. Click **Save** to save the Export Profile.

Modify an Export Profile

To modify an existing export profile:

1. Navigate to **Observability > Performance Management > Profile Management > Export Profiles**.
2. Select the **Export Profiles** tab.
3. In the export profiles list, click on the export profile to edit.
4. Make required changes to the export profile settings.
5. Click **Save**.

Delete an Export Profile

To delete an existing export profile:

1. Navigate to **Observability > Performance Management > Profile Management > Export Profiles**.
2. Select the **Export Profiles** tab.
3. Click the **Delete** icon corresponding to the export profile you want to delete.
4. Confirm the deletion when prompted.

Configure Overrides for Statistics in Export Profiles

The Ribbon Application Management Platform (RAMP) Performance Management (PM) service lets you configure overrides for individual performance statistics in an Export Profile. With an override, you can enable or disable export of the statistic or change the frequency at which it is exported.

Refer to [Define Statistics to Export](#) for information on how to create an Export Profile.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Profile Management > Export Profiles**.
3. Select the Export Profile for which you want to define overrides.
4. In the **Statistics** table select the checkbox next to one or more statistics for which you want to configure an override.
5. Select **Override Selected** from the **Select Action** menu. Configure the following information in the **Override Statistic(s) for Export** window:

Field	Description
Export	Enable or disable the export of the selected statistic(s) using the Export toggle.
Export Frequency	Define how often the system performs exports of the performance data, from the dropdown list.
Granularity	To define the contents (time slices) of the exported files, set select All , 1 hour or 1 day .
Export Locations	Select a location to which to export data, from the list of available export locations.

6. Click **Save** to save the configuration changes.

Configure Performance Management Export Options

In this section:

- [Configure Management Settings for All Nodes and Per Profile Export](#)
- [Configure Management Settings for Per Node Export](#)
- [Configure Management Settings for Common Export Options](#)

The Ribbon Application Management Platform (RAMP) Performance Management (PM) service provides administrative options that apply to performance data you export. The settings are divided into three categories based on the types of export to which they apply: all node and per profile exports, per-node exports, and common options. The options define the date/time format in exported files, timestamp format, and the number of export profiles users can create. You can also configure the data retention period for exported files and export frequency intervals. The PM service also lets you specify whether to raise traps in case of PM issues and whether to compress (zip) export files.

Configure Management Settings for All Nodes and Per Profile Export

Use the **All Nodes / Per Profile Export Configuration** area to configure settings that apply when you select **All Nodes Export** or **Per Profile Export** as the export type. Refer to [Configure Export Type](#) for more details on selecting the export type.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Administration**.
3. In the **All Nodes / Per Profile Export Configuration** section under **Exporter**, enter the following information:

Field	Description
Use GMT for Timestamp	Choose to use GMT for timestamps. By default, it is disabled. Note: This setting applies only if you select All Nodes Export as the export type.
All Node Export File Name Date Time Format	Select the date/time format to use in the export file names. The default setting is -yyyy-MM-dd-HH-mm . This option applies when you select All Nodes Export or Per Profile Export as the export type.
All Node Export Data Row Date Time Format	Select the date/time format to use in each exported data row. Select a format from the available options. The default setting is yyyy/MM/dd HH:mm:ss (24-hour format). This option applies when you select All Nodes Export or Per Profile Export as the export type.

Field	Description
Use Beginning For Timestamp	Enable this option to use the beginning time as the timestamp in export data. When disabled, the timestamp is the end time. For example, data exported for the time interval between 10:00 AM and 10:15 AM marks 10:00 AM in the timestamp if you enable this option, and 10:15 AM if you don't enable this option. Note: If you enable Use Beginning For Timestamp, for RAMP to correctly determine the beginning of interval timestamp, you must set the collection interval on the device and the PM Data Collection interval to identical values.
Use ZIP For Export Files	Enable this option to zip export files.
Export File Supplier ID	Specify the supplier ID to be used in the export file. The default value is SONUS. Note: This setting applies only if you select All Nodes Export as the export type.
Maximum number of user created export profiles	Configure the maximum number of export profiles that users can create. The value range is between 1 and 50. The default value is 35. Note Before a migration, if the number of profiles on RAMP is greater than 35, Ribbon recommends increasing the value to 50.

- Click **Save**.

Configure Management Settings for Per Node Export

Use the **Per Node Export Configuration** section to configure settings that apply when you select **Per Node Export** as the export type. Refer to [Configure Export Type](#) for more details on selecting the export type.

Note

For Per Node Export if there is high latency between RAMP and the external export locations, update the parameter `com.rbbn.pm.export.numOfScpThreads` in the `/opt/sonus/pm/data/pm_config.properties` file to `5` and restart file copier service as insight user using the command `/opt/sonus/pm/bin/fileCopierService stop; /opt/sonus/pm/bin/fileCopierService start`.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Administration**.
3. In the **Per Node Export Configuration** section under **Exporter**, enter the following information:

Field	Description
Per Node Export File Name Date Time Format	Select the date/time format to use in the export file names. The default setting is -yyyy-MM-dd-HH-mm-IntervalMIN .
Per Node Export Date Time Format	Select the date/time format to use in each exported data row. The default setting is yyyy/MM/dd HH:mm:ss .

4. Click **Save**.

Configure Management Settings for Common Export Options

Use the **Common Export Configuration** section to configure settings that apply for all export types. Refer to [Configure Export Type](#) for more details on selecting the export type.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Administration**.
3. In the **Common Export Configuration** area under **Exporter**, enter the following information:

Field	Description
Send Trap For Faults	Enable this option to send traps when faults occur during PM data export.
Export Look Back Interval	Specify the number of export frequency intervals to look back at to determine how much data to export, assuming no override is done. This applies either when exporting stats for the first time, or after a period when exporting is enabled but does not take place due to data not being collected successfully or due to RAMP downtime. The default value is 5. Note: Export Look Back Interval value must be greater than 0. Note: Export Look Back Interval is not applicable when Export All Nodes is enabled.
Delay export of data by one interval	Ribbon recommends that you delay data export in large networks containing more than 100 devices so that the exported files contain all the collected data. In large networks, data collection takes longer and export can trigger before collection is complete, which results in data loss. If you enable this option, data export will be delayed for one collection interval.

Field	Description
Use Sub Type in file name	Enable this option to include a sub type in the export file names. By default it is disabled.
Use Sub Type in exported SBX7K file names	Enable this option to include SBX7K statistics and file names. By default it is disabled.
Exported files retention period in days	Specify the number of days exported files must be retained when export files are stored locally. For retaining uncompressed files Ribbon recommends setting the retention period up to 3 days. Retaining uncompressed files for more than 3 days results in 100% disk usage.
Maximum number of user created export profiles	Configure the maximum number of export profiles that users can create. The value range is between 1 and 50. The default value is 35. Note Before migration if the number of profiles on EMS is greater than 35 then Ribbon recommends increasing the value to 50.
Export GSX cluster profile ID	Enable this option to include the cluster profile ID to the exported GSX files. This is applicable only for per node export. By default it is disabled.

- Click **Save**.

Reordering Exported PM CSV Files

The Ribbon Application Management Platform (RAMP) Performance Management (PM) service supports reordering columns in the exported performance statistics CSV files for All Node Export and Per Node Export.

Note

Reorder the columns only under the supervision of Global Product Support (GPS).

Note

Ensure there are no spaces between the column names while editing the column order property file.

Note

For statistics defined in this property file, only the columns that are defined are exported.

Note

If you incorrectly enter a column in the reordering file `exportColOrder.properties`/
`perNodeExportColOrder.properties`, PM export fails for the column.

Prerequisite

Super User [privileges](#) for Performance Management.

Reorder Exported PM CSV Files

Use this procedure to reorder columns in exported CSV files.

Start

1. Log on to RAMP as admin user.
2. Change to insight user:

```
sudo su - insight
```

3. Perform one of the following:
 - a. All Node or Per Profile Export:
 - i. Edit the file:

```
/opt/sonus/pm/data/exportColOrder.properties
```

For example:

```
Ss7RouteStats=NODE_ID,TIMESTAMP,ROUTE_STATUS_INDEX,SS7_ROUTE_NAME,SS7_ROUTE_T  
YPE,SS7_ROUTE_STATE,ROUTE_CONGESTION_LEVEL
```

Modified output:

```
Ss7RouteStats=TIMESTAMP,NODE_ID,ROUTE_STATUS_INDEX,SS7_ROUTE_NAME,SS7_ROUTE_T  
YPE,SS7_ROUTE_STATE,ROUTE_CONGESTION_LEVEL
```

b. Per Node Export:

i. Edit the file:

```
/opt/sonus/pm/data/perNodeExportColOrder.properties
```

For example:

```
Ss7RouteStats=NODE_ID,TIMESTAMP,ROUTE_STATUS_INDEX,SS7_ROUTE_NAME,SS7_ROUTE_T  
YPE,SS7_ROUTE_STATE,ROUTE_CONGESTION_LEVEL
```

Modified output:

```
Ss7RouteStats=TIMESTAMP,NODE_ID,ROUTE_STATUS_INDEX,SS7_ROUTE_NAME,SS7_ROUTE_T  
YPE,SS7_ROUTE_STATE,ROUTE_CONGESTION_LEVEL
```

4. Save the file.

Note

The column reordering takes effect only from the next export. You need not restart RAMP.

Note

PM statistics order is updated in the exported CSV file as per the metadata provided if it is not included in the property file.

Exported PM CSV Files column Order Post upgrade Rollback Procedure

The Ribbon Application Management Platform (RAMP) allows you to rollback the column order for the exported PM CSV files after an upgrade.

After you upgrade RAMP, the export column order property files of the previous build are saved in the `/opt/sonus/pm/data` directory as `exportColOrder.properties.old` and `perNodeExportColOrder.properties.old`.

The column order property files shipped with the new build are saved in the same directory as `exportColOrder.properties.orig` and `perNodeExportColOrder.properties.orig`. The default `exportColOrder.properties` contains the merged columns from the old and original files.

Start

1. Log on to the RAMP CLI as admin user.

2. Change to insight user:

```
sudo su - insight
```

3. To rollback all node export property file:

```
cp -p /opt/sonus/pm/data/exportColOrder.properties.old /opt/sonus/pm/data/
exportColOrder.properties
chown insight:insight /opt/sonus/pm/data/exportColOrder.properties
```

4. To rollback to per node export property file:

```
cp -p /opt/sonus/pm/data/perNodeExportColOrder.properties.old /opt/sonus/pm/data/
perNodeExportColOrder.properties
chown insight:insight /opt/sonus/pm/data/perNodeExportColOrder.properties
```

Restoring Column Order for Exported PM CSV Files

The Ribbon Application Management Platform (RAMP) allows you to restore the column order for the exported PM CSV files after migration.

Use this procedure to restore the column order during migration.

Start

1. Before migration, take a back of the EMS `perNodeExportColOrder.properties` and `exportColOrder.properties`.
2. After you complete the migration, copy the above files to the directory `/opt/sonus/pm/data` as `cust_perNodeExportColOrder.properties` and `cust_exportColOrder.properties`.
3. Log in as insight user and use `restoreExportColumnOrder.py` to restore the `pernodexport` properties:

```
python38 /opt/sonus/pm/sbin/restoreExportColumnOrder.py /opt/sonus/pm/data/
cust_perNodeExportColOrder.properties /opt/sonus/pm/data/
perNodeExportColOrder.properties
```

4. You can restore the all node export properties by using `restoreExportColumnOrder.py` as `insight` user.

```
python38 /opt/sonus/pm/sbin/restoreExportColumnOrder.py /opt/sonus/pm/data/
cust_exportColOrder.properties /opt/sonus/pm/data/exportColOrder.properties
```

Backlog Collection of SBC, MRFP, and PSX Performance Management Data

In this section:

- [Collect and Export of Backlog Data during RAMP Downtime](#)
- [Collect and Export of Backlog Data for Network Downtime](#)

If a Ribbon Application Management Platform (RAMP) experiences a failover, switchover, upgrade, or network failure, RAMP may lose the performance management data. In such scenarios, you can collect and export the backlog data from the nodes to RAMP to maintain all historical data.

Use this section to collect performance management (PM) backlog data for RAMP downtime and network downtime.

Note

SOAP API for SBC Core is supported only while migrating from EMS to RAMP. Greenfield deployments for RAMP do not support configuring SBC Core using SOAP API as they are deprecated and removed in future releases. Instead, use the REST Proxy to configure SBC Core.

Collect and Export of Backlog Data during RAMP Downtime

If RAMP is down during a switchover, failover, or upgrade, then during this time, the backlog data accumulates on the device type. Once it is back online, RAMP collects this backlog data and exports it from the node(s).

Note

FTP based performance management backlog collection files for RAMP **downtime** are stored at `/opt/sonus/ems/weblogic/sonusEms/data/pm_archive/<node name>`

Note

Set similar intervals for both the export and the collection of data schedules. For example, if the collection interval is 5 minutes, then set the export interval to 0 minutes, 5 minutes, 15 minutes, one hour, and one day.

Collect and Export of Backlog Data for Network Downtime

When RAMP and the other devices are up and running, but you lose connectivity between them, the backlog data accumulates on the individual device.

RAMP collects these Backlog files after the network is up and restores connectivity.

The backlog data is exported to RAMP from the node(s) as follows:

For Single Node

- Once you restore connectivity between RAMP and a single node, RAMP exports backlog data for that node alone.

- Two sets of data; backlog aggregate export files and older aggregate export files, generate for the node type.

For Multiple Nodes

- Once you restore connectivity between RAMP and multiple nodes, RAMP exports backlog data from all the multiple nodes.
- RAMP collects backlog data for each node.
- New sets of backlog aggregate data files are available for each node.

To enable the collection of backlog files, refer to [Configure Performance Management Collection Options](#).

Backlog Files

RAMP accumulates all the backlog data in .csv format and generates a .tar file in every given interval.

Note

FTP based performance management backlog collection files for **network downtime** are stored at /opt/sonus/ems/weblogic/sonusEms/data/pm_archive/<node name>

The format of the backlog file name is as follows:

```
<statsname>-<dateformat>-<export frequency>.csv
```

For example,

```
InsightHostUsageStats-2023-05-12-10-55-5MIN.csv
```

Alarms

RAMP generates two [Performance Management Backlog Alarms](#) if any of the following occurs:

- Generation of Performance Statistics tar file fails.
- Performance management backlog file exports.

Assign Collection and Export Profiles

In this section:

- [Assign a Collection Profile to a Node or Cluster](#)
- [Assign an Export Profile to a Node or Cluster](#)
- [Enable Statistics Collection](#)
- [Enable Statistics Export](#)

The Ribbon Application Management Platform (RAMP) Performance Management (PM) service lets you assign the collection and export profiles to nodes or clusters. Once you assign a profile the **device uses the assigned profile settings to determine how to collect or export performance data**. The PM service also allows you to enable or disable collection and export profiles as a whole in addition to allowing you to enable and disable individual statistics within a profile. Refer to [Define Statistics to Collect](#) and [Configure Export Profiles](#) for more information on enabling individual statistics within a profile.

Use the procedures in this section to assign profiles to devices and to enable or disable profiles.

Assign a Collection Profile to a Node or Cluster

The PM service assigns a collection profile to every device registered on RAMP by default.

Use the following procedures to view the current assignment and change it if necessary.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Profile Management > Assignment**
3. Select the **Collection Assignments** tab.
All the devices registered on RAMP are listed along with their default assigned collection profiles.
4. To modify the collection profile assignment, select the checkbox next to a node or cluster and select **Modify Selected** from the **Actions** menu.
5. In the **Modify Selected** window, select a different profile from the **Collection Profile** list.
6. Click **Save** to save your change.

Assign an Export Profile to a Node or Cluster

The PM service assigns an export profile to every device registered on RAMP by default.

Use the following procedures to view the current assignment and change it if necessary.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Profile Management > Assignment**
3. Select the **Export Assignments** tab.
4. All the devices registered on RAMP are listed along with their default assigned export profiles.
5. To modify the export profile assignment, select the checkbox next to a node or cluster and select **Modify Selected** from the **Actions** menu.
6. In the **Modify Selected** window, select a different profile from the **Export Profile** list.
7. Click **Save** to save your change.

Enable Statistics Collection

Use the following procedures to enable or disable statistics collection for a node or cluster.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Profile Management > Assignment**
3. Select the **Collection Assignments** tab.
All the devices registered on RAMP are listed along with their default assigned collection profiles.
4. Use the **Enabled** toggle to enable or disable collecting performance statistics for a node or cluster.

Enable Statistics Export

Use the following procedures to enable or disable statistics export for a node or cluster.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Profile Management > Assignment**
3. Select the **Export Assignments** tab.
All the devices registered on RAMP are listed here, along with their default assigned export profiles.
4. Use the **Export Status** toggle to enable or disable exporting performance statistics for a node or cluster.

Define Data Retention Periods

Retaining performance statistics can require significant storage space depending on the size of your network. By default, the PM service retains interval data for one week and aggregate hourly and daily data for four weeks. To manage data retention, the Ribbon Application Management Platform (RAMP) Performance Management (PM) service lets you specify how long to retain each type of performance statistic.

Use the following procedure to modify the retention periods for one or more performance statistics.

Prerequisite

You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Data Retention**.
3. Select one or more statistics types by clicking the adjacent checkboxes.
4. Click **Edit** in the **Select Action** menu.
5. In the **Update Retention Time** window, enter values for the following:
 - Retention Time for Interval Data
 - Retention Time for Hourly Aggregated Data
 - Retention Time for Daily Aggregated Data
6. Click **Save**.

Working with Reports

Related articles:

- [Customize Report Templates](#)
- [Creating and Downloading Reports](#)

The Ribbon Application Management Platform (RAMP) allows you to view historical performance reports in a graphical or tabular format, based on a report template you select. You can run a performance management report to retrieve a set of statistics data from a specified device, for a specific date range, and with a selected level of granularity. The created reports are available for download in both CSV and PDF formats.

To generate reports in Performance Management:

- Create templates to specify which statistics to include in the report.
- Create reports based on a template. You can add additional criteria for the report, like the device for which you want the report and the granularity.
- Run and download reports for devices to which you have access.

Customize Report Templates

In this section:

- [Create a Report Template](#)
- [Modify a Report Template](#)
- [Delete a Report Template](#)

Before you can run individual reports, you must create a report template for each type of report that you want to run. A report template specifies the type of device, the statistics group, and which individual metrics within that group (up to 10) to include in the report.

RAMP does not provide default templates, they must be configured.

Create a Report Template

Use the following procedures to create a report template.

Prerequisite

You require Operator or Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Reporting > Templates**.
3. Click **Add Template**.
4. Enter the following information:

Field	Description
Template Name	Enter a name for the report template.
Node Type	Select the type of node for which the template is intended.
Stats Name	Select the statistics group for which the template is intended. Select the statistics group that provides important information for the devices in your network.
Column Selection	Select the individual metrics within the selected statistics group (up to 10) to include in the report. From the Available columns list, select the column names to include in the template by moving it to the Selected columns list using the arrow buttons.

5. Click **Save** to save the template.

Modify a Report Template

To edit an existing report template:

1. Navigate to **Observability > Performance Management > Reporting > Templates**.
2. In the templates list, click on the template to edit.
3. Make required changes to the template settings.
4. Click **Save**.

Delete a Report Template

To delete an existing report template:

1. Navigate to **Observability > Performance Management > Reporting > Templates**.
2. Click the Delete icon corresponding to the template you want to delete.
3. Confirm the deletion when prompted.

Creating and Downloading Reports

In this section:

- [Create a Performance Report](#)
 - [Modify a Performance Report](#)
 - [Delete a Performance Report](#)
- [Run and Download Reports](#)

Create specific reports to evaluate a specific set of performance statistics for a selected device. You can create a report for a specific node, for the required time period, based on a pre-defined template. You can also set the granularity for the data.

Create a Performance Report

Use the following procedure to create a report.

Prerequisites

- You require Operator or Super User [privileges](#) for Performance Management to create reports and report templates.
- Enable data collection for every device that you want to generate reports for (requires Super User privileges).
- Create a report template. Refer to [Customize Report Templates](#) for information on how to create a report template.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Reporting > Reports**.
3. Click **Add Report**.
4. Enter the following information:

Field	Description
Report Name	Enter a name for the report.
Date Range	Set a date range for which you want the statistics.

Field	Description
Granularity	In the report, when you select the granularity value, statistics are displayed for each period of time dictated by the granularity setting. For example, setting the granularity to 1 hour results in a table with statistics displayed for 1 hour intervals for the specified date range.
Node Type	Select the type of device for which you want to create a report. Note: The node type cannot be edited after creating and saving the report.
Template	Select a template from the list of templates available for the selected node type. Use separate templates for nodes and clusters. Note: The template selection cannot be edited after creating and saving the report.
Node/Cluster	Depending on the node type selected, either a Node or Cluster list appears. Select the node or cluster for which you want to add the report.
Report Columns	Select the required report columns. Options appear based on your node/cluster selection.

5. Click **Save**.

Modify a Performance Report

To edit an existing report:

1. Navigate to **Observability > Performance Management > Reporting > Reports**.
2. In the reports list, click on the report to edit.
3. Make required changes to the report settings.
4. Click **Save**.

Delete a Performance Report

To delete an existing report:

1. Navigate to **Observability > Performance Management > Reporting > Reports**.
2. Select **Delete** from the Action list for the report you want to delete.
3. Confirm the deletion when prompted.

Run and Download Reports

Generate and download performance reports to view and monitor performance statistics in graphical and tabular forms. The reports are available for download in both PDF and CSV formats.

Prerequisites

- You require Operator or Super User level [privileges](#) for Performance Management to run and download reports.

- Enable data collection for every device that you want to generate reports (requires Super User privileges). Refer to [Assign Collection and Export Profiles](#) for more information on enabling collection profiles.

Note

The new CE name is not populated in saved reports, if you change the CE name post an SBC upgrade.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Reporting > Reports**.
3. To generate a report, select **Run** in the **action** list corresponding to the report you want to generate. The "Edit Report" window displays the statistics report in the form of a chart and statistics table. Depending on the report, you might have to make a selection of a run-time option, such as a node name or another parameter, before the report runs.
4. To download this report, click **Download** and select either **Download PDF** or **Download CSV** depending on the report format you want.
5. Click **Save** to exit the **Edit Report** window.

Define Performance Thresholds

In this section:

- [Create a Threshold](#)
- [Modify a Threshold](#)
- [Delete a Threshold](#)

Related articles:

- [Aggregate Thresholds](#)

The threshold alarm feature provides a way for users of the Ribbon Application Management Platform (RAMP) to receive alarm notifications when the values of selected performance measures cross specified threshold values. When these values are crossed, RAMP triggers alarms within the fault management service with a severity level specified in the threshold configuration.

For a selected performance measure, you can:

- Specify values for triggering and clearing alarms. If the trigger value is higher than the clearing value then the threshold is classified as a 'high threshold' and is triggered if a polled value is higher than the trigger value. It is cleared if the polled value is lower than the clearing value. If the trigger value is lower than the clearing value then the threshold is classified as a 'low threshold' and will be triggered if a polled value is lower than the trigger value and will be cleared if the polled value is higher than the clearing value.
- Specify the severity of the alarm that's generated as the result of a threshold crossing.

The RAMP Performance Management (PM) service allows you to specify a threshold for a performance measure. This provides a method to generate alarms of different severities for different performance measures. For example, you can specify that if a given performance measure rises above 70%, the system sends a minor alarm.

Thresholds apply only to performance metrics that are enabled in a device's collection profile. The [sonusEmsV2RisingEventNotification](#) alarm is raised when thresholds are triggered and the [sonusEmsV2FallingEventNotification](#) alarm is raised to clear the previous alarm when thresholds are cleared.

Create a Threshold

Use the following procedure to create a threshold for a selected performance metric.

Prerequisites

- Enable data collection for devices that you require thresholds. Refer to [Assign Collection and Export Profiles](#) for more information on enabling collection profiles.
- You require Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Thresholding**.
3. To create a new Threshold, click **Add Threshold**.
4. In the **Create Threshold** window, select the type of node for which you want to configure a threshold from the **Node type** list.
5. Select the category that contains the metric for which you want to configure a threshold from the **Category** list.
6. Select the statistic to check for the threshold from the **Name** list.
7. Enter a **Trigger** value for the threshold. RAMP triggers an alarm when the trigger value is crossed.
8. Enter a **Clearing** value for the threshold. RAMP clears the alarm once the clearing value is crossed.
9. Select the severity level of the alarm from the options available in the **Severity** list.
10. Enable the **Notify on clearing threshold crossed** toggle to enable notification when a measurement crosses the falling threshold.
11. Enable the **Enabled** toggle to enable the threshold.
12. Click **Save** to save the Threshold.

Modify a Threshold

To edit an existing threshold:

1. Navigate to **Observability > Performance Management > Thresholding**.
2. In the thresholds list, click on the threshold you want to edit.
3. Make required changes to the threshold information.
4. Click **Save**.

Delete a Threshold

To delete an existing threshold:

1. Navigate to **Observability > Performance Management > Thresholding**.
2. Select the checkbox next to the threshold you want to delete.
3. Select **Delete** from the **Bulk Action** list.
4. Confirm the deletion when prompted.

Aggregate Thresholds

The Ribbon Application Management Platform (RAMP) Performance Management (PM) service can be configured to aggregate threshold alarms raised by managed entities, such as trunk groups, to the node level. This reduces the number of alarms. RAMP raises a single alarm for the node rather than individual alarms for each trunk group that crosses a threshold value.

This alarm contains a path to a file that contains details of trunk groups (or other entities) which crossed the threshold value. This alarm is kept alive and updated as long as there are one or more entities beyond the

configured thresholds. The alarm is cleared and the file is deleted after all entities go below the threshold clearing mark.

Use the following procedure to enable aggregating threshold alarms.

Prerequisite

Super User [privileges](#) for Performance Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Performance Management > Administration**.
3. Under **Thresholding Configuration**, select the **Enable aggregation of thresholds** checkbox.
4. Click **Save**.

Exported Statistics

In this section:

- [DSC Statistics](#)
- [DSI Statistics](#)
- [GSX Statistics](#)
- [Insight Statistics](#)
- [PSX Statistics](#)
- [SBC Core Statistics](#)
 - [MRFP Statistics](#)
 - [SBC 5400 and SBC SWe Statistics](#)
 - [SBC 7000 Statistics](#)
 - [SBC CNF Statistics](#)
 - [SLB Statistics](#)
- [SBC Edge Statistics](#)
- [SGX4000 Statistics](#)

This section lists and explains all the performance management statistics available on the Ribbon Application Management Platform (RAMP).

You can export PM statistics only in CSV format. You can configure export statistics parameters. Refer to [Configure Performance Management Export Options](#) for more information on how to configure the format of CSV file parameters.

DSC Statistics

In this section:

- [DSCADNSCTPPATHSTATS](#)
- [DSCADNSTATS](#)
- [DSCCPUSTATS](#)
- [DSCDISKSTATS](#)
- [DSCGATEWAYSCREENINGSTATS](#)
- [DSCGWACCMTP3RXSTATS](#)

- [DSCGWACCMTP3TXSTATS](#)
- [DSCGWACCSCCPRXSTATS](#)
- [DSCGWACCSCCPTXSTATS](#)
- [DSCINAPGWSTATS](#)
- [DSCIWFSTATS](#)
- [DSCLINKSCTPPATHSTATS](#)
- [DSCLINKSETSTATS](#)
- [DSCLINKSTATS](#)
- [DSCM3UAASPCTPPATHSTATS](#)
- [DSCM3UAASPSTATS](#)
- [DSCMEMORYSTATS](#)
- [DSCMSGSTATS](#)
- [DSCNODESTATS](#)
- [DSCNPGWSTATS](#)
- [DSCOVLSTATS](#)
- [DSCREALMACCSTATS](#)
- [DSCRLSTATS](#)
- [DSCROUTESETSTATS](#)
- [DSCRTASUBTRSTATS](#)
- [DSCRTATRANSSTATS](#)
- [DSCSCTPIPGBLSTATS](#)
- [DSCSUAASPCTPPATHSTATS](#)
- [DSCSUAASPSTATS](#)
- [DSCSYSMONSTATS](#)
- [DSCSYSTEMSTATS](#)
- [DCTPSSTATS](#)

DSCADNSCTPPATHSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
NUM_PATH_STATE_CHANGES	COUNTER	false	Num Path state changes	true

DSCADNSTATS

ADN indicates Adjacent Diameter Node (ADN). For more information, refer to [Adjacent Diameter Node Data Measurements](#).

Column Name	Column Type	Index	Description
INSTANCE	STRING	TRUE	Instance
REQUEST_RX	COUNTER	FALSE	Request Received
REQUEST_TX	COUNTER	FALSE	Requests sent

Column Name	Column Type	Index	Description
ANSWERS_RX	COUNTER	FALSE	Answers Received
ANSWERS_TX	COUNTER	FALSE	Answers Sent
ERRORS_RX	COUNTER	FALSE	Errors Received
REDIRECTS_RX	COUNTER	FALSE	Redirects Received
MSG_RX	COUNTER	FALSE	Messages Received
MSG_TX	COUNTER	FALSE	Messages Sent
BYTES_RX	COUNTER	FALSE	Bytes Received
BYTES_TX	COUNTER	FALSE	Bytes Sent
AVRG_TX_QUEUE_TIME	COUNTER	FALSE	Average Transmit Queue Time
TX_QUEUE_TIME_SAMPLE_SIZE	COUNTER	FALSE	Transmit Queue Time Sampled Messages
AVRG_TRNSCTN_TIME	COUNTER	FALSE	Average Transaction Time
TRNSCTN_TIME_SAMPLE_SIZE	COUNTER	FALSE	Transaction Time Sampled Messages
AVRG_TX_QUEUE_DEPTH	COUNTER	FALSE	Average Transmit Queue Depth
TX_QUEUE_DEPTH_SAMPLE_SIZE	COUNTER	FALSE	Transmit Queue Depth Sample Size
SCTP_RXN_DATA_CHUNKS	COUNTER	FALSE	SCTP Retransmission Data Chunks

DSCCPUSTATS

Note

DSCCPUSTATS is available only if the DM `EMS12.0.0-DSC18.0.0-DM1.0.0-pkg.tar.gz` is installed on RAMP.

Column name	Column type	Index	Description
INSTANCE	STRING	true	The name of the instance.
SAMPLES	COUNTER	false	The count of samples.
USER_PERCENTAGE	COUNTER	false	The percentage of user.
SYSTEM_PERCENTAGE	COUNTER	false	The percentage of the system.
NICE_PERCENTAGE	COUNTER	false	The percentage of NICE.
IDLE_PERCENTAGE	COUNTER	false	The percentage of IDLE.
USAGE_PERCENTAGE	COUNTER	false	The percentage of usage.
IOWAIT_PERCENTAGE	COUNTER	false	The percentage of IO WAIT.
IRQ_PERCENTAGE	COUNTER	false	The percentage of IRQ.
SOFTIRQ_PERCENTAGE	COUNTER	false	The percentage of SOFTIRQ.
STEAL_PERCENTAGE	COUNTER	false	The percentage of STEAL.
GUEST_PERCENTAGE	COUNTER	false	GUEST percentage
GUEST_NICE_PERCENTAGE	COUNTER	false	The percentage of GUEST NICE.
MAX_USAGE_PERCENTAGE	COUNTER	false	Maximum usage percentage
FIFTEEN_MINUTE_LOAD_AVERAGE	COUNTER	false	The load average in 15 minutes.
MAXFIFTEEN_MINUTELOAD_AVERAGE	COUNTER	false	The maximum load average in 15 minutes.

DSCDISKSTATS

Note

DSCDISKSTATS is available only if the DM EMS12.0.0-DSC18.0.0-DM1.0.0-pkg.tar.gz is installed on RAMP.

Column name	Column type	Index	Description
INSTANCE	STRING	true	The name of the instance.
SAMPLES	COUNTER	false	The count of samples.
DISK_SIZE	COUNTER	false	Size of the partition in Kibibytes.
USED	COUNTER	false	Space used in the partition in Kibibytes.
AVAILABLE	COUNTER	false	Space available in the partition in Kibibytes.
USE_PERCENTAGE	COUNTER	false	The percentage of USE.
QUOTA_PERCENTAGE	COUNTER	false	The percentage of QUOTA.
WRITE_OPS_PER_MINUTE	COUNTER	false	The count of WRITE operations per minute.
READ_OPS_PER_MINUTE	COUNTER	false	The count of READ operations per minute.

DSCGATEWAYSCREENINGSTATS

Column name	Column type	Description
SCREENING_SUCCESS	COUNTER	Number of MSUs successfully screened by GWS, including any redirected MSUs, screening test mode failures, or SCRERR failure overrides.
SCREENING_FAILS	COUNTER	Number of MSUs discarded with logs (paced) by GWS due to any screening table or SCRERR failures. The screening failures are broken down into their associated counts for invalid screening tables and SCRERR.
SCREENING_IGNORES	COUNTER	Number of MSUs discarded without logs (silently) by GWS due to any screening table record failure with next step set to IGNORE. The screening ignores are broken down into their associated counts for invalid screening tables

Column name	Column type	Description
SCREENING_TEST_MODES	COUNTER	Number of MSUs which are not discarded but failed screening due to the screening test mode setting at GWS or on a per screening record basis. Included in the Screening Success overall count.
SCREENING_INVALID_OCs	COUNTER	Number of MSUs discarded by GWS due to the allowed OPCs and Blocked OPCs screening tables. Included in the Screening Fail and Ignore overall count as applicable.
SCREENING_INVALID_DPCS	COUNTER	Number of MSUs discarded by GWS due to the allowed DPCs and Blocked DPCs screening tables. Included in the Screening Fail and Ignore overall count as applicable.
SCREENING_INVALID_SIOs	COUNTER	Number of MSUs discarded by GWS due to the allowed SIOs screening table. Included in the screening fail and Ignore overall count as applicable.
SCREENING_INVALID_AFFECTED_DESTINATIONS	COUNTER	Number of MSUs discarded by GWS due to the affected destinations screening table. Included in the Screening Fail and Ignore overall count as applicable.
SCREENING_INVALID_ISUP_MTs	COUNTER	Number of MSUs discarded by GWS due to the allowed ISUP MTs screening table. Included in the Screening Fail and Ignore overall count as applicable.
SCREENING_INVALID_SCCP_CLG_PAs	COUNTER	Number of MSUs discarded by GWS due to the allowed SCCP CLG PAs screening table. Included in the Screening Fail and Ignore overall count as applicable.
SCREENING_INVALID_SCCP_CLG_DIGITS_PAs	COUNTER	Number of MSUs discarded by GWS due to the allowed SCCP CLG Digits PAs screening table. Included in the Screening Fail and Ignore overall count as applicable.
SCREENING_INVALID_SCCP_TTs	COUNTER	Number of MSUs discarded by GWS due to the allowed SCCP TTs screening table. Included in the Screening Fail and Ignore overall count as applicable.

Column name	Column type	Description
SCREENING_INVALID_SCCP_CLD_DIGITS-PAs	COUNTER	Number of MSUs discarded by GWS due to the allowed SCCP CLD Digits PAs screening table. Included in the Screening Fail and Ignore overall count as applicable.
SCREENING_INVALID_SCCP_CLD_PAs	COUNTER	Number of MSUs discarded by GWS due to the allowed SCCP CLD PAs screening table. Post-GTT table. Included in the Screening Fail and Ignore overall count as applicable.
SCREENING_INVALID_AFFECTED_SCCP_MGMTS	COUNTER	Number of MSUs discarded by GWS due to the affected SCCP Mgmts screening table. Post-GTT. Always 0 as no viable configuration to trigger this failure.
SCREENING_INVALID_TCAP_OP_CODES	COUNTER	Number of MSUs discarded by GWS due to the allowed TCAP Op Codes screening table. Can be post-GTT is assigned following an Allowed SCCP CLD PA record. Included in the Screening Fail and Ignore overall count as applicable.
SCREENING_INVALID_MAP_IMSIs	COUNTER	Number of MSUs discarded by GWS due to the allowed MAP IMSIs screening table. Included in the Screening Fail and Ignore overall count as applicable.
SCRERRs	COUNTER	Number of MSUs which are either passed or discarded by GWS due to an screening configuration error. SCRERRs are logged (paced). Included in the Screening Success and Failure overall count depending on the SCRERR action (configuration override screening success or screening failure).
REDIRECT_TO_PCS_DPC_ORIGINAL	COUNTER	Number of MSUs redirected to a point code (PC) where the DPC remains unchanged. Included in the Screening Success overall count.
REDIRECT_TO_PCS_CPD_OVERRIDE	COUNTER	Number of MSUs redirected to a point code (PC) where the DPC is overridden by the provided attribute value. Included in the Screening Success overall count.
REDIRECT_TO_APPIDS_ORIGINAL	COUNTER	Number of MSUs redirected to an application ID where the original MSU is passed along to a local application if available. Included in the Screening Success overall count.

Column name	Column type	Description
REDIRECT_TO_APPIDS_DUPLICATE	COUNTER	Number of MSUs redirected to an application ID where a duplicate MSU is passed along to a local application if available and the original MSU is routed normally by MTP3 based on its DPC. Included in the Screening Success overall count.

DSCGWACCMTP3RXSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
GWA_MTP3_MSUMSG_RX	COUNTER	false	Gateway MTP3 MSU Message RX	true
GWA_MTP3_OCTETMSG_RX	COUNTER	false	Gateway MTP3 Octet Message RX	true

DSCGWACCMTP3TXSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
GWA_MTP3_MSUMSG_TX	COUNTER	false	Gateway MTP3 MSU Message TX	true
GWA_MTP3_OCTETMSG_TX	COUNTER	false	Gateway MTP3 Octet Message TX	true

DSCGWACCSCCPRXSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
GWA_SCCP_MSUMSG_RX	COUNTER	false	Gateway SCCP MSU Message RX	true
GWA_SCCP_OCTETMSG_RX	COUNTER	false	Gateway SCCP Octet Message RX	true

DSCGWACCSCCPTXSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
GWA_SCCP_MSU_MS G_TX	COUNTER	false	Gateway SCCP MSU Message TX	true
GWA_SCCP_OCTET_ MSG_TX	COUNTER	false	Gateway SCCP Octet Message TX	true

DSCINAPGWSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
GSM_INCOMING_QUE RIES	COUNTER	false	GSM Incoming Queries	true
GSM_INCOMING_OCT ETS	COUNTER	false	GSM Incoming Octets	true
INAP_OUTGOING_QU ERIES	COUNTER	false	INAP Outgoing Queries	true
INAP_OUTGOING_OC TETS	COUNTER	false	INAP Outgoing Octets	true
INAP_INCOMING_RES PONSES	COUNTER	false	INAP Incoming Responses	true
INAP_INCOMING_OCT ETS	COUNTER	false	INAP Incoming Octets	true
INAP_INCOMING_CON NECTS	COUNTER	false	INAP Incoming Connects	true
INAP_INCOMING_CON TINUES	COUNTER	false	INAP Incoming Continues	true
INAP_INCOMING_ERR OR_RESP	COUNTER	false	INAP Incoming Error Response	true

Column Name	Column Type	Index	Description	Aggregated
INAP_INCOMING_UNASSC_RESP	COUNTER	false	INAP Incoming Unassociated Response	true
INAP_QUERY_TIMEOUTS	COUNTER	false	INAP Query Timeouts	true
GSM_INVALID_QUERIES	COUNTER	false	GSM Invalid Queries	true
GSM_INAP_UNAVAILABLE	COUNTER	false	GSM INAP Unavailable	true
GSM_MAP_ERRORS	COUNTER	false	GSM Map Errors	true

DSCIWFSTATS

For more information, refer to [IWF Data Measurements](#).

Column Name	Column Type	Index	Description
INSTANCE	STRING	TRUE	Instance
MAP_INCOMING_MESSAGES	COUNTER	FALSE	MAP Incoming Octets
MAP_OUTGOING_MESSAGES	COUNTER	FALSE	MAP Outgoing Messages
MAP_OUTGOING_OCTETS	COUNTER	FALSE	MAP Outgoing Octets
MAP_TRANSACTIONS	COUNTER	FALSE	MAP Transactions
MAP_TRANSACTIONS_EXPIRED	COUNTER	FALSE	MAP Initiated Transactions Expired
MAP_UNSUPPORTED_OPERATIONS	COUNTER	FALSE	MAP Unsupported Operations
DIAMETER_INCOMING_MESSAGES	COUNTER	FALSE	Diameter Incoming Messages
DIAMETER_INCOMING_OCTETS	COUNTER	FALSE	Diameter Incoming Octets

Column Name	Column Type	Index	Description
DIAMETER_OUTGOING_MESSAGES	COUNTER	FALSE	Diameter Outgoing Messages
DIAMETER_OUTGOING_OCTETS	COUNTER	FALSE	Diameter Outgoing Octets
DIAMETER_TRANSACTIONS	COUNTER	FALSE	Diameter Transactions
DIAMETER_TRANSACTIONS_EXPIRED	COUNTER	FALSE	Diameter Initiated Transactions Expired
DIAMETER_UNSUPPORTED_REQUESTS	COUNTER	FALSE	Diameter Unsupported Requests
CONVERSION_ERRORS	COUNTER	FALSE	Conversion Errors

DSCLINKSCTPPATHSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
LINK_NUM_PATH_STATE_CHANGE	COUNTER	false	Link State Num Path state changes	true

DSCLINKSETSTATS

For more information, refer to [Linkset and Link Data Measurements](#).

Column Name	Column Type	Index	Description
INSTANCE	STRING	TRUE	Instance
MSU_TRANSMITTED	COUNTER	FALSE	MSU's transmitted
MSU_RECEIVED	COUNTER	FALSE	MSU's received
OCTETS_TRANSMITTED	COUNTER	FALSE	MSU's octets transmitted
OCTETS_RECEIVED	COUNTER	FALSE	MSU's octets received
MSU_REC_REQ_GTT	COUNTER	FALSE	MSUs received requiring GTT

Column Name	Column Type	Index	Description
OCTETS_MSU_REQ_GTT	COUNTER	FALSE	MSU octets received for MSUs requiring GTT
DURATION_OF_INACTIVITY	COUNTER	FALSE	Duration of link set inactivity

DSCLINKSTATS

For more information, refer to [Linkset and Link Data Measurements](#).

Column Name	Column Type	Index	Description
INSTANCE	STRING	TRUE	Instance
MSU_TX	COUNTER	FALSE	MSU TX
MSU_RX	COUNTER	FALSE	MSU RX
OCTETS_TX	COUNTER	FALSE	Octets TX
OCTETS_RX	COUNTER	FALSE	Octets RX
OUTAGE_TIME	COUNTER	FALSE	Outage Time
RETRANSMIT_DUE_TO_ERROR	COUNTER	FALSE	Retransmit due to Error
OCT_RETRANSMIT_DUE_TO_ERROR	COUNTER	FALSE	Octet Retransmit due to error
AUTO_CHANGEOVER	COUNTER	FALSE	Automatic Changeover
NEGATIVE_ACK	COUNTER	FALSE	Negative Ack
MAINTENANCE_USAGE	COUNTER	FALSE	Link Maintenance Usage
CONG_L1_DURATION	COUNTER	FALSE	Duration of Level 1 Link Congestion
CONG_L2_DURATION	COUNTER	FALSE	Duration of Level 2 Link Congestion
CONG_L3_DURATION	COUNTER	FALSE	Duration of Level 3 Link Congestion

Column Name	Column Type	Index	Description
ENTERING_CONG_L1_COUNT	COUNTER	FALSE	Event Count for Entering Level 1 Link Congestion
ENTERING_CONG_L2_COUNT	COUNTER	FALSE	Event Count for Entering Level 2 Link Congestion
ENTERING_CONG_L3_COUNT	COUNTER	FALSE	Event Count for Entering Level 3 Link Congestion
PRI0_MSU_DSCRD_DUETO_CONG	COUNTER	FALSE	Priority 0 MSU's Discarded Due to Congestion
PRI1_MSU_DSCRD_DUETO_CONG	COUNTER	FALSE	Priority 1 MSU's Discarded Due to Congestion
PRI2_MSU_DSCRD_DUETO_CONG	COUNTER	FALSE	Priority 2 MSU's Discarded Due to Congestion
PRI3_MSU_DSCRD_DUETO_TXBUF	COUNTER	FALSE	Priority 3 MSU's Discarded Due to Full Transmit Buffer
LINK_ACTIVE_TIME	COUNTER	FALSE	Link Active Time
LINK_AVAILABLE_TIME	COUNTER	FALSE	Link Available Time
NEAR_END_FORCED_UNAVAILABLE	COUNTER	FALSE	Near End Forced Link Unavailable
FAR_END_MGMT_INHIBIT	COUNTER	FALSE	Number of Far-End Management Inhibits
MSU_REC_REQ_GTT	COUNTER	FALSE	MSU received requiring GTT
OCTET_MSU_REC_REQ_GTT	COUNTER	FALSE	Octets received for MSUs requiring GTT
FAIL_PROVE_AUTO_CHANGE_OVER	COUNTER	FALSE	Failed to prove in after an automatic changeover
DUR_OF_DECLARED_FAILURE_ALL	COUNTER	FALSE	Duration of declared signaling link failure
OUTPUT_DELAY_AVG	COUNTER	FALSE	Output delay average

Column Name	Column Type	Index	Description
OUTPUT_DELAY_SAMPLE_SIZE	COUNTER	FALSE	,Output delay sample size
TB_OCCUPANCY_AVG	COUNTER	FALSE	TB occupancy average
TB_OCCUPANCY_SAMPLE_SIZE	COUNTER	FALSE	TB occupancy sample size
LINK_CAPACITY	COUNTER	FALSE	Link capacity
SCTP_RXN_DATA_CHUNKS	COUNTER	FALSE	Link Sctp Retransmission Data Chunks

DSCM3UAASPCTPPATHSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
M3UA_ASP_NUM_PATH_STATE_CHAN	COUNTER	false	M3UA ASP Num Path state changes	true

DSCM3UAASPSTATS

For more information, refer to [SG ASP SCTP Association Data Measurements](#).

Column Name	Column Type	Index	Description
INSTANCE	STRING	TRUE	Instance
MSG_TX_TO_M3UA	COUNTER	FALSE	Msgs TX to M3UA ASP
MSG_RX_FROM_M3UA	COUNTER	FALSE	Msgs RX from M3UA ASP
BYTES_TX_TO_M3UA	COUNTER	FALSE	Bytes TX to M3UA ASP
BYTES_RX_TO_M3UA	COUNTER	FALSE	Bytes RX to M3UA ASP
MSGS_DISCARDED_TX	COUNTER	FALSE	Msgs Discarded TX to M3UA ASP
MSGS_DISCARDED_RX	COUNTER	FALSE	Msgs Discarded RX from M3UA ASP

Column Name	Column Type	Index	Description
M3UA_ASP_OUTAGE_TIME	COUNTER	FALSE	M3UA ASP Outage Time
SCTP_RXN_DATA_CHUNKS	COUNTER	FALSE	M3UA ASP Sctp Retransmission Data Chunks

DSCMEMORYSTATS

Note

DSCMEMORYSTATS is available only if the DM EMS12.0.0-DSC18.0.0-DM1.0.0-pkg.tar.gz is installed on RAMP.

Column name	Column type	Index	Description
INSTANCE	STRING	true	The name of the instance.
SAMPLES	COUNTER	false	The count of samples.
MEMTOTAL	COUNTER	false	Total amount of physical RAM in kilobytes.
MEMAVAILABLE	COUNTER	false	The memory available
MEMAVAILABLE_PERCENTAGE	COUNTER	false	The percentage of memory available.
SRECLAIMABLE	COUNTER	false	SRE CLAIMABLE
SUNRECLAIM	COUNTER	false	Amount of the slab that cannot be reclaimed.
MEMFREE	COUNTER	false	Free memory
MEMFREE_PERCENTAGE	COUNTER	false	The percentage free memory.
MINIMUM_MEMFREE_PERCENTAGE	COUNTER	false	The percentage of minimum memory free.
MAX_PROC_MEM_USAGE_PERCENTAGE	COUNTER	false	The percentage of maximum process memory usage.

Column name	Column type	Index	Description
MAX_PROCESS_MEMORY_USAGE_PID	COUNTER	false	The maximum process memory usage PID.

DSCMSGSTATS

For more information, refer to [DSC Message Counters](#).

Column Name	Column Type	Index	Description
INSTANCE	STRING	TRUE	Instance
MSG_CUSTOM_1	COUNTER	FALSE	Custom Message 1
MSG_CUSTOM_2	COUNTER	FALSE	Custom Message 2
MSG_CUSTOM_3	COUNTER	FALSE	Custom Message 3
MSG_CUSTOM_4	COUNTER	FALSE	Custom Message 4
MSG_CUSTOM_5	COUNTER	FALSE	Custom Message 5
MSG_CUSTOM_6	COUNTER	FALSE	Custom Message 6
MSG_CUSTOM_7	COUNTER	FALSE	Custom Message 7
MSG_CUSTOM_8	COUNTER	FALSE	Custom Message 8
MSG_CUSTOM_9	COUNTER	FALSE	Custom Message 9
MSG_CUSTOM_10	COUNTER	FALSE	Custom Message 10

DSCNODESTATS

For more information, refer to [DSC Node Counters](#).

Column Name	Column Type	Index	description
ANSWERS_RX	COUNTER	FALSE	Answers Received
ANSWERS_TX	COUNTER	FALSE	Answers Sent
AVRG_PROC_TIME	COUNTER	FALSE	Average Processing Time

Column Name	Column Type	Index	description
AVRG_QUEUEING_TIME	COUNTER	FALSE	Average Queueing Time
AVRG_TRNSCTN_TIME	COUNTER	FALSE	Average Transaction time
BYTES_RX	COUNTER	FALSE	Bytes Received
BYTES_TX	COUNTER	FALSE	Bytes Sent
INSTANCE	STRING	TRUE	Instance
MSGs_RX	COUNTER	FALSE	Messages Received
MSGs_TX	COUNTER	FALSE	Messages Sent
PROC_TIME_SAMPLE_SIZE	COUNTER	FALSE	Processing Time Sampled Messages
QUEUEING_TIME_SAMPLE_SIZE	COUNTER	FALSE	Queueing Time Sampled Messages
REQUEST_TIMEOUT	COUNTER	FALSE	Requests Timeouts
REQUESTS_RX	COUNTER	FALSE	Request Received
REQUESTS_TX	COUNTER	FALSE	Requests sent
SCTP_RXN_DATA_CHUNKS	COUNTER	FALSE	SCTP Retransmission Data Chunks
TRNSCTN_TIME_SAMPLE_SIZE	COUNTER	FALSE	Transaction Time Sampled Messages

DSCNPGWSTATS

For more information, refer to [NPGW Data Measurements](#).

Column Name	Column Type	Index	Description	CanAggregate
INSTANCE	STRING	TRUE	Instance	FALSE
MTP3_INCOMING_MSGS	COUNTER	FALSE	Number of MSUs received from the SS7/IP network at the NP Gateway from MTP3.	TRUE

Column Name	Column Type	Index	Description	CanAggregate
MTP3_INCOMING_OCTETS	COUNTER	FALSE	Number of octets received from the SS7/IP network at the NP Gateway from MTP3.	TRUE
PSX_NP_TISUP_QUERIES	COUNTER	FALSE	Number of NP Triggerless ISUP queries sent to the PSX.	TRUE
PSX_NP_TISUP_RESPONSES	COUNTER	FALSE	Number of NP Triggerless ISUP responses received from the PSX.	TRUE
PSX_NP_TISUP_NOT_PRTD	COUNTER	FALSE	Number of IAMs which are not ported as per the PSX responses.	TRUE
PSX_NP_TISUP_PRTD_PFX	COUNTER	FALSE	Number of IAMs which are ported via the IAM prefix option as per the PSX responses.	TRUE
PSX_NP_TS_PRTD_REL	COUNTER	FALSE	Number of IAMs which are ported via the REL return option as per the PSX responses.	TRUE
PSX_NP_TS_UNASS_RES	COUNTER	FALSE	Number of NP Triggerless ISUP responses received from the PSX that cannot be matched to pending queries. Likely due to expiry.	TRUE
PSX_NP_TS_QUERY_TMT	COUNTER	FALSE	Number of NP queries which did not receive a response in the configurable timer interval.	TRUE
PSX_NP_TS_IVD_INTCP	COUNTER	FALSE	Number of invalid intercepted messages for NP Triggerless ISUP.	TRUE
PSX_NP_TISUP_ERRORS	COUNTER	FALSE	Number of IAMs which could not complete the PSX NP database dip (excluding timeouts). This includes PSX down, PSX queue full, and NP response digit processing errors such as out of bounds.	TRUE
PSX_NP_TISUP_AVG_RES	COUNTER	FALSE	Average response time for a NP Triggerless ISUP query to the PSX.	TRUE
PSX_NP_TP_AVG_RESMPL	COUNTER	FALSE	Sample size of the average response time for a NP Triggerless ISUP query to the PSX.	TRUE

DSCOVLSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
REQUESTS	COUNTER	false	Requests	true
REQUESTS_REJECTED	COUNTER	false	Requests Rejected	true
REQUESTS_DROPPED	COUNTER	false	Requests Dropped	true
ANSWERS	COUNTER	false	Answers	true
ANSERS_DROPPED	COUNTER	false	Answers Dropped	true
MESSAGES_DROPPED	COUNTER	false	Message Dropped	true
OVERLOAD_L1_SECONDS	COUNTER	false	Overload L1 seconds	true
OVERLOAD_L1_COUNT	COUNTER	false	Overload L1 count	true
OVERLOAD_L2_SECONDS	COUNTER	false	Overload L2 Seconds	true
OVERLOAD_L2_COUNT	COUNTER	false	Overload L2 count	true
OVERLOAD_L3_SECONDS	COUNTER	false	Overload L3 Seconds	true
OVERLOAD_L3_COUNT	COUNTER	false	>Overload L3 count	true

DSCREALMACCSTATS

For more information, refer to [Realm Accounting](#).

Column Name	Column Type	Index	Description
INSTANCE	STRING	TRUE	Instance

Column Name	Column Type	Index	Description
INCOMING_REQUESTS	COUNTER	FALSE	Incoming Requests
OUTGOING_REQUESTS	COUNTER	FALSE	Outgoing Requests
INCOMING_ANSWERS_2XXX	COUNTER	FALSE	Incoming Answers UTD
OUTGOING_ANSWERS_2XX X	COUNTER	FALSE	Outgoing Answers UTD
INCOMING_ANSWERS_UTD	COUNTER	FALSE	Incoming Answers UTD
OUTGOING_ANSWERS_UTD	COUNTER	FALSE	Outgoing Answers UTD
INCOMING_ANSWERS_REDIRE CT	COUNTER	FALSE	Incoming Answers Redirect
OUTGOING_ANSWERS_REDIRE CT	COUNTER	FALSE	Outgoing Answers Redirect
INCOMING_ANSWERS_OTHE R	COUNTER	FALSE	Incoming Answers Other
OUTGOING_ANSWERS_OTH ER	COUNTER	FALSE	Outgoing Answers Other
RETRANSMIT_REQUESTS	COUNTER	FALSE	Retransmit Requests
REJECTED_REQUESTS_FILT ER	COUNTER	FALSE	Rejected Requests Filtering
REJECTED_REQUESTS_ING RS_FILTER	COUNTER	FALSE	Rejected Requests Ingress Filtering
REJECTED_REQUESTS_OTH ER	COUNTER	FALSE	Rejected Requests Other
TIMEOUT_REQUESTS	COUNTER	FALSE	Timeout Requests
DISCARD_ANSWERS	COUNTER	FALSE	Discarded Answers

DSCRLSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
REQUEST_IN	COUNTER	false	Request In	true
REQUEST_OUT	COUNTER	false	Request Out	true
ANSWER_IN	COUNTER	false	Answers In	true
ANSWER_OUT	COUNTER	false	Answers out	true
MESSAGE_IN	COUNTER	false	Messages In	true
MESSAGE_OUT	COUNTER	false	Messages Out	true
BYTES_IN	COUNTER	false	Bytes In	true
BYTES_OUT	COUNTER	false	Bytes out	true
AVERAGE_QUEUE_TIME	COUNTER	false	Average Queue time	true
QUEUE_TIME_SAMPLE_SIZE	COUNTER	false	Queue time sample size	true
AVERAGE_QUEUE_DEPTH	COUNTER	false	Average Queue depth	true
QUEUE_DEPTH_SAMPLE_SIZE	COUNTER	false	Queue depth sample size	true

DSCROUTESETSTATS

For more information, refer to [Destination Data Measurements](#).

Column Name	Column Type	Index	Description
INSTANCE	STRING	TRUE	Instance
PR0_DISCARD_DUE_TO_CONGESTION	COUNTER	FALSE	Priority 0 MSUs discarded due to route set congestion

Column Name	Column Type	Index	Description
PR1_DISCARD_DUETO_CONGESTION	COUNTER	FALSE	Priority 1 MSUs discarded due to route set congestion
PR2_DISCARD_DUETO_CONGESTION	COUNTER	FALSE	Priority 2 MSUs discarded due to route set congestion
DUR_OF_L1_ROUTESET_CONG	COUNTER	FALSE	Duration of Level 1 Route Set Congestion
DUR_OF_L2_ROUTESET_CONG	COUNTER	FALSE	Duration of Level 2 Route Set Congestion
DUR_OF_L3_ROUTESET_CONG	COUNTER	FALSE	Duration of Level 3 Route Set Congestion

DSCRTASUBTRSTATS

The statistics on round-trip delays for each Diameter and SS7 request type is compiled.

RTA indicates Round-Trip Accounting. SUBTR indicates Sub-transaction. Sub-transaction is an outbound transaction that attempts to complete the inbound Transaction. More than one sub-transactions may be necessary to complete a Transaction.

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	TRUE	Instance Name of the statistics output.	FALSE
SUCCESS_DELAY	COUNTER	FALSE	Average delay for sub-transactions that resulted in success result.	TRUE
SUCCESS_MSGS	COUNTER	FALSE	Number of messages included in the calculation for DSC_RTA_SUBTR_SUCCESS_DELAY	TRUE
SUCCESS_O100	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_SUCCESS_MSGS with delay value of at least 100 ms, but less than 500 ms	TRUE
SUCCESS_O500	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_SUCCESS_MSGS with delay value of at least 500 ms, but less than 1000 ms	TRUE

Column Name	Column Type	Index	Description	Aggregated
SUCCESS_O1000	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_SUCCESS_M SGS with delay value of at least 1000 ms	TRUE
REDIRECT_DELAY	COUNTER	FALSE	Average delay for sub-transactions that resulted in DIAMETER_REDIRECT_INDICATION result	TRUE
REDIRECT_MSGS	COUNTER	FALSE	Number of messages included in the calculation for DSC_RTA_SUBTR_REDIRECT_DELAY	TRUE
REDIRECT_O100	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_REDIRECT_M SGS with delay value of at least 100 ms, but less than 500 ms	TRUE
REDIRECT_O500	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_REDIRECT_M SGS with delay value of at least 500 ms, but less than 1000 ms	TRUE
REDIRECT_O1000	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_REDIRECT_M SGS with delay value of at least 1000 ms	TRUE
UTD_DELAY	COUNTER	FALSE	Average delay for sub-transactions that resulted in DIAMETER_UNABLE_TO_DELIVER result	TRUE
UTD_MSGS	COUNTER	FALSE	Number of messages included in the calculation for DSC_RTA_SUBTR_UTD_DELAY	TRUE
UTD_O100	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_UTD_MSGS with delay value of at least 100 ms, but less than 500 ms	TRUE

Column Name	Column Type	Index	Description	Aggregated
UTD_O500	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_UTD_MSGS with delay value of at least 500 ms, but less than 1000 ms	TRUE
UTD_O1000	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_UTD_MSGS with delay value of at least 1000 ms	TRUE
OTHER_DELAY	COUNTER	FALSE	Average delay for sub-transactions that resulted in a result other than success or DIAMETER_UNABLE_TO_DELIVER	TRUE
OTHER_MSGS	COUNTER	FALSE	Number of messages included in the calculation for DSC_RTA_SUBTR_OTHER_DELAY	TRUE
OTHER_O100	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_OTHER_MSGS with delay value of at least 100 ms, but less than 500 ms	TRUE
OTHER_O500	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_OTHER_MSGS with delay value of at least 500 ms, but less than 1000 ms	TRUE
OTHER_O1000	COUNTER	FALSE	Number of messages within DSC_RTA_SUBTR_OTHER_MSGS with delay value of at least 1000 ms	TRUE

DSCRTATRANSSTATS

The statistics on round-trip delays for each Diameter and SS7 request type is compiled.

TRANS indicates transaction. A transaction consists of a request message and its corresponding reply message as viewed from the incoming Adjacent Diameter Node (ADN).

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	TRUE	Instance Name of the statistics output.	FALSE
SUBTRANS	COUNTER	FALSE	Number of sub-transactions issued	TRUE

Column Name	Column Type	Index	Description	Aggregated
SUCCESS_DELAY	COUNTER	FALSE	Average delay for transactions that resulted in success result. This is the average round-trip delay measured on a sub-transaction where the response has a result code of 2xxx.	TRUE
SUCCESS_MESSAGES	COUNTER	FALSE	Number of messages included in the calculation for DSC_RTA_TRANS_SUCCESS_DELAY (Success Delay measurement).	TRUE
SUCCESS_O100	COUNTER	FALSE	Number of messages within DSC_RTA_TRANS_SUCCESS_MESSAGES with delay value of at least 100 ms, but less than 500 ms	TRUE
SUCCESS_O500	COUNTER	FALSE	Number of messages within DSC_RTA_TRANS_SUCCESS_MESSAGES with delay value of at least 500 ms, but less than 1000 ms	TRUE
SUCCESS_O1000	COUNTER	FALSE	Number of messages within DSC_RTA_TRANS_SUCCESS_MESSAGES with delay value of at least 1000 ms	TRUE
UTD_DELAY	COUNTER	FALSE	Average delay for transactions that resulted in DIAMETER_UNABLE_TO_DELIVER result	TRUE
UTD_MSGS	COUNTER	FALSE	Number of messages included in the calculation for DSC_RTA_TRANS_UTD_DELAY	TRUE
UTD_O100	COUNTER	FALSE	Number of messages within DSC_RTA_TRANS_UTD_MSGS with delay value of at least 100 ms, but less than 500 ms	TRUE
UTD_O500	COUNTER	FALSE	Number of messages within DSC_RTA_TRANS_UTD_MSGS with delay value of at least 500 ms, but less than 1000 ms	TRUE
UTD_O1000	COUNTER	FALSE	Number of messages within DSC_RTA_TRANS_UTD_MSGS with delay value of at least 1000 ms	TRUE

Column Name	Column Type	Index	Description	Aggregated
OTHER_DELAY	COUNTER	FALSE	Average delay for transactions that resulted in a result other than success or DIAMETER_UNABLE_TO_DELIVER	TRUE
OTHER_MSGS	COUNTER	FALSE	Number of messages included in the calculation for DSC_RTA_TRANS_OTHER_DELAY	TRUE
OTHER_O100	COUNTER	FALSE	Number of messages within DSC_RTA_TRANS_OTHER_MSGS with delay value of at least 100 ms, but less than 500 ms	TRUE
OTHER_O500	COUNTER	FALSE	Number of messages within DSC_RTA_TRANS_OTHER_MSGS with delay value of at least 500 ms, but less than 1000 ms	TRUE
OTHER_O1000	COUNTER	FALSE	Number of messages within DSC_RTA_TRANS_OTHER_MSGS with delay value of at least 1000 ms	TRUE

DSCSCTPIPGBLSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
SCTP_PACKETS_IN	COUNTER	false	Sctp Packets In	true
SCTP_PACKETS_OUT	COUNTER	false	Sctp packets out	true
SCTP_ACTIVE_ESTAB S	COUNTER	false	Sctp active estabs	true
SCTP_PASSIVE_ESTA BS	COUNTER	false	Sctp passive estabs	true
SCTP_ABORTEDS	COUNTER	false	Sctp aborted	true
SCTP_SHUTDOWNS	COUNTER	false	Sctp shutdown	true
SCTP_OUT_OF_BLUES	COUNTER	false	Sctp out of blues	true

Column Name	Column Type	Index	Description	Aggregated
SCTP_CHECKSUM_ERRORS	COUNTER	false	Sctp checksum error	true
SCTP_OUT_CTRL_CHUNKS	COUNTER	false	Sctp out control chunks	true
SCTP_OUT_ORDER_CHUNKS	COUNTER	false	Sctp out order chunks	true
SCTP_OUT_UNORDER_CHUNKS	COUNTER	false	Sctp out unordered chunks	true
SCTP_IN_CTRL_CHUNKS	COUNTER	false	Sctp in control chunks	true
SCTP_IN_ORDER_CHUNKS	COUNTER	false	Sctp in order chunks	true
SCTP_IN_UNORDER_CHUNKS	COUNTER	false	Sctp in order chunks	true
SCTP_FRAG_USER_MSGS	COUNTER	false	Sctp frag user msgs	true
SCTP_REASM_USER_MSGS	COUNTER	false	SCTP Reasm user msg	true
IP_IN_PACKETS	COUNTER	false	Ip in packets	true
IP_OUT_PACKETS	COUNTER	false	Ip out packets	true
IP_IN_DISCARDS	COUNTER	false	Ip In discards	true
IP_OUT_DISCARDS	COUNTER	false	Ip out discards	true
IP_RX_UNKNOWN_PROTOCOL	COUNTER	false	Ip RX unknown proto	true

DSCSUAASPSCTPPATHSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false

Column Name	Column Type	Index	Description	Aggregated
SUA_ASP_NUM_PATH_STATE_CHAN	COUNTER	false	SUA ASP Num Path state changes	true

DSCSUAASPSTATS

For more information, refer to [SG ASP SCTP Association Data Measurements](#).

Column Name	Column Type	Index	Description
INSTANCE	STRING	TRUE	Instance
SUA_ASP_TX_MSG	COUNTER	FALSE	Msgs TX to SUA ASP
SUA_ASP_RX_MSG	COUNTER	FALSE	Msgs RX from SUA ASP
SUA_ASP_TX_BYTES	COUNTER	FALSE	Bytes TX to SUA ASP
SUA_ASP_RX_BYTES	COUNTER	FALSE	Bytes RX to SUA ASP
SUA_ASP_DISCARD_MSG_TX	COUNTER	FALSE	Msgs Discarded TX to SUA ASP
SUA_ASP_DISCARD_MSG_RX	COUNTER	FALSE	Msgs Discarded RX from SUA ASP
SUA_ASP_OUTAGE_TIME	COUNTER	FALSE	SUA ASP Outage Time
SUA_ASP_SCTP_RXN_DATA_TRUNKS	COUNTER	FALSE	SUA ASP Sctp Retransmission Data Chunks

DSCSYSMONSTATS

For more information, refer to [SYSMON Data Measurements](#).

Column Name	Column Type	Index	Description
INSTANCE	STRING	TRUE	Instance
CORE_1_USAGE	COUNTER	FALSE	CORE_1_USAGE
CORE_2_USAGE	COUNTER	FALSE	CORE_2_USAGE
CORE_3_USAGE	COUNTER	FALSE	CORE_3_USAGE

Column Name	Column Type	Index	Description
CORE_4_USAGE	COUNTER	FALSE	CORE_4_USAGE
CORE_5_USAGE	COUNTER	FALSE	CORE_5_USAGE
CORE_6_USAGE	COUNTER	FALSE	CORE_6_USAGE
CORE_7_USAGE	COUNTER	FALSE	CORE_7_USAGE
CORE_8_USAGE	COUNTER	FALSE	CORE_8_USAGE
CORE_9_USAGE	COUNTER	FALSE	CORE_9_USAGE
CORE_10_USAGE	COUNTER	FALSE	CORE_10_USAGE
CORE_11_USAGE	COUNTER	FALSE	CORE_11_USAGE
CORE_12_USAGE	COUNTER	FALSE	CORE_12_USAGE
CORE_13_USAGE	COUNTER	FALSE	CORE_13_USAGE
CORE_14_USAGE	COUNTER	FALSE	CORE_14_USAGE
CORE_15_USAGE	COUNTER	FALSE	CORE_15_USAGE
CORE_16_USAGE	COUNTER	FALSE	CORE_16_USAGE
CORE_17_USAGE	COUNTER	FALSE	CORE_17_USAGE
CORE_18_USAGE	COUNTER	FALSE	CORE_18_USAGE
CORE_19_USAGE	COUNTER	FALSE	CORE_19_USAGE
CORE_20_USAGE	COUNTER	FALSE	CORE_20_USAGE
CORE_21_USAGE	COUNTER	FALSE	CORE_21_USAGE
CORE_22_USAGE	COUNTER	FALSE	CORE_22_USAGE
CORE_23_USAGE	COUNTER	FALSE	CORE_23_USAGE
CORE_24_USAGE	COUNTER	FALSE	CORE_24_USAGE

Column Name	Column Type	Index	Description
CORE_25_USAGE	COUNTER	FALSE	CORE_25_USAGE
CORE_26_USAGE	COUNTER	FALSE	CORE_26_USAGE
CORE_27_USAGE	COUNTER	FALSE	CORE_27_USAGE
CORE_28_USAGE	COUNTER	FALSE	CORE_28_USAGE
CORE_29_USAGE	COUNTER	FALSE	CORE_29_USAGE
CORE_30_USAGE	COUNTER	FALSE	CORE_30_USAGE
CORE_31_USAGE	COUNTER	FALSE	CORE_31_USAGE
CORE_32_USAGE	COUNTER	FALSE	CORE_32_USAGE
USAGE_READ_COUNT	COUNTER	FALSE	USAGE_READ_COUNT

DSCSYSTEMSTATS

For more information, refer to [System and Slot Data Measurements](#).

Column Name	Column Type	Index	Description
INSTANCE	STRING	TRUE	Instance
ORIG_MSU	COUNTER	FALSE	Originated MSU
TERM_MSU	COUNTER	FALSE	Terminated MSU
THRU_SWITCH_MSU	COUNTER	FALSE	Thru-switch MSU
OCTETS_ORIG	COUNTER	FALSE	Originated MSU Octets
OCTETS_TERM	COUNTER	FALSE	Terminated MSU Octets
OCTETS_THRU	COUNTER	FALSE	Thru-switch MSU Octets
GTT_RECEIVED	COUNTER	FALSE	GTT Received
GTT_PERFORMED	COUNTER	FALSE	GTT Performed

Column Name	Column Type	Index	Description
GTT_PERFORMED_DEFAULT_PC	COUNTER	FALSE	GTT Performed Default PC List
GTT_NOT_PERFORMED	COUNTER	FALSE	Gtt not performed
CRITICAL_ALARMS	COUNTER	FALSE	Critical Alarms
MAJOR_ALARMS	COUNTER	FALSE	Major Alarms
MINOR_ALARMS	COUNTER	FALSE	Minor Alarms
MSU_DISCARD_INVALID_DPC	COUNTER	FALSE	MSUs Discarded due to invalid DPC
MSU_DISCARD_INVALID_SIO	COUNTER	FALSE	MSUs Discarded due to invalid SIO
MTP_RESTART_INITIATED	COUNTER	FALSE	Number of MTP restarts initiated
GTT_BAD_MSU	COUNTER	FALSE	GTT bad MSU
GTT_NO_RULE_FOUND_CALLED	COUNTER	FALSE	GTT no rule found called
GTT_NO_ADDR_FOUND_CALLED	COUNTER	FALSE	GTT No Address Found - called
GTT_IGNORED	COUNTER	FALSE	Gtt Ignored
NODE_PROC_TIME_AVG	COUNTER	FALSE	Node processing time average
NODE_PROC_TIME_SAMPLE_SIZE	COUNTER	FALSE	Node Processing Time Sample Size
CROSS_STP_TIME_AVG	COUNTER	FALSE	Cross STP time average
CROSS_STP_TIME_SAMPLE_SIZE	COUNTER	FALSE	Cross STP time sample size
NODE_PROC_TIME_SAMPLE_F95	COUNTER	FALSE	Node Processing time 95th percentile failure

Column Name	Column Type	Index	Description
CROSS_STP_TIME_SAMPLE_F95	COUNTER	FALSE	Cross STP time 95th percentile failure
GTT_NO_RULE_FOUND_CALLING	COUNTER	FALSE	GTT No Rule Found- Calling
GTT_NO_ADDR_FOUND_CALLING	COUNTER	FALSE	GTT No Address Found Calling
GTT_NO_RULE_FOUND_OPC	COUNTER	FALSE	GTT No Rule Found - OPC
IMF_SENT	COUNTER	FALSE	IMF Sent
IMF_DISCARDED	COUNTER	FALSE	IMF Discarded
UP_TIME	COUNTER	FALSE	The system's uptime in seconds. Note The counter is available only if the DM EMS12.0.0-DSC18.0.0-DM1.0.0-pkg.tar.gz is installed on Ribbon Application Management Platform (RAMP).

DSCTPSSTATS

Column Name	Column Type	Index	Description	Aggregated
INSTANCE	STRING	true	Instance	false
INSTANCE_TOTAL_TRANS_RECV	COUNTER	false	Instance total trans Recieved	true
SYSTEM_TOTAL_TRANS_RECV	COUNTER	false	System total trans Recieved	true
INSTANCE_TPS_SAMPLE_SIZE	COUNTER	false	Instance Tps Sample Size	true

Column Name	Column Type	Index	Description	Aggregated
SYSTEM_TPS_SAMPLE_SIZE	COUNTER	false	System Tps Sample Size	true
INSTANCE_AVERAGE_TPS	COUNTER	false	Instance Average TPS	true
SYSTEM_AVERAGE_TPS	COUNTER	false	System Average TPS	true
DURATION_L1_TPS_THRESHOLD	COUNTER	false	Duration of L1 TPS threshold	true
DURATION_L2_TPS_THRESHOLD	COUNTER	false	Duration of L2 TPS threshold	true
DURATION_L3_TPS_THRESHOLD	COUNTER	false	Duration of L3 TPS threshold	true
DRTN_INSTANCE_TPS_THRESHOLD_REUSE	COUNTER	false	Duration Instance TPS threshold overuse	true
DURN_SYS_L1_TPS_THRESHOLD	COUNTER	false	Duration of System L1 TPS Threshold	true
DURN_SYS_L2_TPS_THRESHOLD	COUNTER	false	Duration of System L2 TPS Threshold	true
DURN_SYS_L3_TPS_THRESHOLD	COUNTER	false	Duration of System L3 TPS Threshold	true
DRTN_SYSTEM_TPS_THRESHOLD_REUSE	COUNTER	false	Duration of System TPS Threshold overuse	true

DSI Statistics

In this section:

- [DSIHostFsUsageStats](#)
- [DSIHostStats](#)

DSIHostFsUsageStats

Column Name	Column Type	Index	Description
PATH_NAME	STRING	Yes	The File System Path Name
USAGE	INTEGER	No	The File System Usage in percentage

DSIHostStats

Column Name	Column Type	Index	Description
CPU_AVG_USAGE	INTEGER	No	The average CPU usage percentage (rounded to the nearest integer) averaged over a 5 minute interval. The averaging is performed at the end of the interval. The CPU usage is calculated using this formula: (user time + kernel time)/(user time + kernel time + IO wait time + idle time) * 100. The sampling period is 5 seconds.
MEM_USAGE	INTEGER	No	The average host physical memory usage percentage (rounded to the nearest integer) averaged over a 5 minute interval. The averaging is performed at the end of the interval. The usage value is calculated by dividing total in use memory by total physical memory in the system. The sampling period is 5 seconds.
SWAP_SPACE_USAGE	INTEGER	No	The average host swap space usage percentage (rounded to the nearest integer) averaged over a 5 minute interval. The averaging is performed at the end of the interval. The usage value is calculated by dividing total in use swap space by total available swap space. The usage value is represented as a percentage and is rounded to the nearest integer!. The sampling period is 5 seconds.
PEAK_CPU_USAGE	INTEGER	No	Peak CPU usage percentage (round up to integer) during the interval.
PEAK_MEM_USAGE	INTEGER	No	Peak host physical memory usage percentage during the interval.
PEAK_SWAP_SPACE_USAGE	INTEGER	No	Peak host swap space usage percentage during the interval.

Note

DSIHostStats statistics collection supports only 5 minutes hard-coded polling interval and the statistics are collected every 5 minutes from DSI. The DSIHostStats statistics collection interval cannot be changed.

GSX Statistics

In this section:

- [AccountingSummaryStats](#)
- [CallCountStats](#)
- [CongestionIntervalStats](#)
- [GatewayCallStats](#)
- [GSXDspSlotStats](#)
- [GSXHpcIntervalStats](#)
- [GSXImStatusStats](#)
- [GSXMlppIntervalStats](#)
- [GSXPeakCallStat](#)
- [GSXSipHpcIntervalStats](#)
- [GSXSipHpcLimitStats](#)
- [GSXSipSigPortTlsStats](#)
- [GSXSipSigPortTlsStatusStats](#)
- [GSXSlotDspResIntervalStats](#)
- [GSXSonicBusUsageIntervalStats](#)
- [Ss7DestinationStats](#)
- [Ss7LinkStats](#)
- [Ss7RouteStats](#)
- [GSXSysCallDspResIntervalStats](#)
- [GSXSysDspResHighestUsageStats](#)
- [GSXSysDspResIntervalStats](#)
- [GsxTgIntervalStats](#)
- [IPMTRGIntervalStats](#)
- [IPTrunkGroupIntervalStats](#)
- [PNSEnetStats](#)
- [SoftswitchStats](#)
- [SystemStats](#)
- [TrunkGroupIntervalStats](#)
- [TrunkGroupStats](#)

AccountingSummaryStats

Column Name	Column Type	Index	Description	canAggregate
ACCT_NUM_CALL_ATTEMPTS	COUNTER64	No	This field contains the difference between the last polled Number of Call Attempts value and the current polled value.	true
ACCT_NUM_CALL_COMPLETIONS	COUNTER64	No	This field contains the difference between the last polled Number of Successful Call Completions value and the current polled value.	true
ACCT_NUM_CALL_ATTEMPT_FAILURES	COUNTER64	No	This field contains the difference between the last polled Number of Unsuccessful Call Attempts value and the current polled value.	true
ACCT_NUM_BUSY_HOUR_ATTEMPTS	INTEGER	No	The Average BHCA rate in the last one hour or last statistic reset.	true
ACCT_NUM_CALL_ATTEMPT_RATE	INTEGER	No	The call arrival rate in calls/sec in the last one minute interval prior to Ribbon Application Management Platform (RAMP) polling the GSX. The GSX computes and maintains the rate (value) using the following method: Rate = calls/60 with the remainder (modulo) added to the total. For example, if 30 calls occur in the last minute of data collection, 30/60 would yield a rate of 0. A range of 31 90 calls yields an average of 1, and a range of 91 150 yields 2/sec, etc.	true

Column Name	Column Type	Index	Description	canAggregate
ACCT_NUM_AVG_CALL_DURATION	INTEGER	No	The Average Call Duration in seconds. Duration is measured from service established to call disconnect. This average only accounts for completed calls, not calls in progress or call attempts. Note This is an average that uses all calls established since the last reboot or MNS switchover.	true
ACCT_NUM_CALL_ATTEMPT_BLOCKED	COUNTER64	No	This field contains the difference between the last polled Number of Calls which were blocked/screened value and the current polled value.	true

CallCountStats

Column Name	Column Type	Index	Description	canAggregate
PEG_COUNTS_SHELF_INDEX	INTEGER	Yes	Identifies the target shelf to obtain the call counters.	false
PEG_COUNTS_SLOT_INDEX	INTEGER	Yes	Identifies the target slot.	false
PEG_COUNTS_ATT_EMPTS	COUNTER	No	Indicates the number of call attempts on this card.	true
PEG_COUNTS_COMPLETIONS	COUNTER	No	Indicates the total number of completed call attempts on this card.	true
PEG_COUNTS_ACTIVE_CALLS	GAUGE	No	Indicates the number of managed calls active on this card. In a managed call, a card maintains all resources for the call including the assignment of the GCID (global call identifier). A card may also simply provide resources for other calls. The non-managed calls are not reflected in this count.	true

Column Name	Column Type	Index	Description	canAggregate
PEG_COUNTS_STABLE_CALLS	GAUGE	No	Indicates the number of stable managed calls active on this card. In a managed call, a card maintains all resources for the call including the assignment of the GCID (global call identifier). A card may also simply provide resources for other calls. These non-managed calls are not reflected in this count.	true

Note

File based collection (SFTP) includes slots that are enabled and ACTIVE.
 SNMP collection includes slots that are enabled irrespective of the status (ACTIVE or STANDBY).

CongestionIntervalStats

Column Name	Column Type	Index	Description	canAggregate
MC1_COUNT	COUNTER	No	The number of transitions into MC1.	true
MC1_TOTAL_TIME	COUNTER	No	The sum of time spent in MC1 in seconds.	true
MC2_COUNT	COUNTER	No	The number of transitions into MC2.	true
MC2_TOTAL_TIME	COUNTER	No	The sum of time spent in MC2 in seconds.	true
MC3_COUNT	COUNTER	No	The number of transitions into MC3.	true
MC3_TOTAL_TIME	COUNTER	No	The sum of time spent in MC3 in seconds.	true
OVERLOAD_REJECTS	COUNTER	No	The number of calls rejected by NRM due to GSX congestion.	true
AVG_CALL_RATE	GAUGE	No	The system average call arrival rate.	true

Column Name	Column Type	Index	Description	canAggregate
PEAK_CALL_RATE	GAUGE	No	The system peak call arrival rate.	true
DS_OVERLOAD_REJECTS	COUNTER	No	The number of calls rejected by DS due to PSX congestion.	true
INTERVAL_ARRIVALS	COUNTER	No	The number of call arrivals.	true

GatewayCallStats

Note

Ribbon recommends to configure the collection frequency to an hour or more for networks containing more than 50 GSXs.

Column Name	Column Type	Index	Description	canAggregate
GW_NAME	STRING	No	Name of the remote Gateway.	false
GW_IP	IPADDRESS	Yes	IP Address of the remote Gateway.	false
GW_NUM_ACTIVE_CALLS	INTEGER	No	Number of active calls between local and remote Gateway.	true
GW_NUM_ACTIVE_CALLS_TO	INTEGER	No	Number of active calls to this remote Gateway.	true
GW_NUM_ACTIVE_CALLS_FROM	INTEGER	No	Number of active calls from this remote Gateway.	true
GW_FROM_TOTAL_CALLS	COUNTER64	No	The total number of calls originated by the remote on this link.	true
GW_FROM_CALL_RATE	INTEGER	No	The number of calls/sec processed by the GWFE in the last minute on the link which was originated by the remote.	true

Column Name	Column Type	Index	Description	canAggregate
GW_TO_TOTAL_CALLS	COUNTER64	No	The total number of calls originated locally on this link.	true
GW_TO_CALL_RATE	INTEGER	No	The number of calls/sec processed by the GWFE in the last minute on the link which was originated locally.	true
GW_BHA	INTEGER	No	The accumulated call attempts to this gateway in the previous hour.	true
GW_IPV6	IPV6ADDRESS	Yes	IPv6 address of the remote Gateway.	false
GW_IPVERSION	INTEGER	Yes	IP address type of the Gateway signaling link.	false

GSXDspSlotStats

Column Name	Column Type	Index	Description	canAggregate
SHELF_INDEX	INTEGER	Yes	Shelf index for this table	false
SLOT_INDEX	INTEGER	Yes	Slot index for this table	false
G711EC_TOTAL	INTEGER	No	Total number of G711 with Echo Cancellation resources available on this slot	true
G711NOECHOCANCEL	INTEGER	No	Total number of G711 resources available on this slot	true
HDLC_TOTAL	INTEGER	No	Total number of HDLC resources available on this slot	true
TONE_TOTAL	INTEGER	No	Total number of Tones resources available on this slot	true
G729AB_TOTAL	INTEGER	No	Total number of G729A+B resources available on this slot	true
G711EC_UTILIZATION	INTEGER	No	Percentage utilization of G711 Echo canceller resources on this slot	true

Column Name	Column Type	Index	Description	canAggregate
G711EC_ALLOC_FAILURES	INTEGER	No	Percentage of G711 Echo canceller resources allocation failures on this slot	true
G711UTILIZATION	INTEGER	No	Percentage utilization of G711 resources on this slot	true
G711ALLOC_FAILURES	INTEGER	No	Percentage of G711 resources allocation failures on this slot	true
HDLC_UTILIZATION	INTEGER	No	Percentage utilization HDLC resources on this slot	true
HDLC_ALLOC_FAILURES	INTEGER	No	Percentage of HDLC resources allocation failures on this slot	true
TONE_UTILIZATION	INTEGER	No	Percentage utilization of Tone resources on this slot	true
TONE_ALLOC_FAILURES	INTEGER	No	Percentage of Tone resources allocation failures on this slot	true
G729AB_UTILIZATION	INTEGER	No	Percentage utilization of G729A+B resources on this slot	true
G729AB_ALLOC_FAILURES	INTEGER	No	Percentage of G729A+B resources allocation failures on this slot	true
PACKET_OUTAGE_TOTAL	INTEGER	No	Total number of packet outages exceeding the user-specified threshold on a CNS or SPS. The user can reset the object.	true
PACKET_OUTAGE_INTERVAL	INTEGER	No	Number of packet outages exceeding the user-specified threshold since the last PacketOutageThresholdExceeded trap was generated on a CNS or SPS.	true
G7231TOTAL	INTEGER	No	Total number of G723.1 resources available on this slot	true
G7231UTILIZATION	INTEGER	No	Percentage utilization of G7231 resources on this slot	true

Column Name	Column Type	Index	Description	canAggregate
G7231ALLOC_FAILURES	INTEGER	No	Percentage of G7231 resources allocation failures on this slot	true
G726TOTAL	INTEGER	No	Total number of G726 resources available on this slot	true
G726UTILIZATION	INTEGER	No	Percentage utilization of G726 resources on this slot	true
G726ALLOC_FAILURES	INTEGER	No	Percentage of G726 resources allocation failures on this slot	true
G711_COMPRESS_TOTAL	INTEGER	No	Total number of compression resources available on this slot	true
COMPRESSION_UTILIZATION	INTEGER	No	Percentage utilization of compression resources on this slot	true
COMPRESSION_ALLOC_FAILURES	INTEGER	No	Percentage of compression resources allocation failures on this slot	true
CONF_TOTAL	INTEGER	No	Total number of conference resources available on this slot	true
CONF_UTILIZATION	INTEGER	No	Percentage utilization of conference resources on this slot	true
CONF_ALLOC_FAILURES	INTEGER	No	Percentage of conference resources allocation failures on this slot	true
CONF_PARTICIPANT_TOTAL	INTEGER	No	Total number of participant resources available on this slot	true
CONF_PARTICIPANT_UTILIZATION	INTEGER	No	Percentage utilization of participant resources on this slot	true
CONF_PARTICIPANT_ALLOC_FAIL	INTEGER	No	Percentage of participant resources allocation failures on this slot	true
ILBC_TOTAL	INTEGER	No	Total number of iLBC resources available on this slot	true

Column Name	Column Type	Index	Description	canAggregate
ILBC_UTILIZATION	GAUGE	No	Percentage utilization of iLBC resources on this slot	true
ILBC_ALLOC_FAILURES	INTEGER	No	Percentage of iLBC resources allocation failures on this slot	true

Note

File based collection (SFTP) includes slots that are enabled and ACTIVE.
 SNMP collection includes slots that are enabled irrespective of the status (ACTIVE or STANDBY).

GSXHpcIntervalStats

Column Name	Column Type	Index	Description
PSTN_EGRESS_CALLS	COUNTER	No	The number of HPC calls going out to PSTN trunks.
IP_IN_INGRESS_CALLS	COUNTER	No	The number of HPC calls going out on internal IPTGs (Inbound IPTGs).
IP_IN_EGRESS_CALLS	COUNTER	No	The number of HPC calls coming in on the internal IPTGs (Outbound IPTGs).
IP_EX_INGRESS_CALLS	COUNTER	No	The number of HPC calls going out on external IPTGs (Inbound IPTGs).
IP_EX_EGRESS_CALLS	COUNTER	No	The number of HPC calls coming in on the external IPTGs (Outbound IPTGs) for the specified interval.
NO_ROUTE_CALLS	COUNTER	No	The number of HPC calls that cannot be connected to any route in the route list.
CQ_Q_ATTEMPTS	COUNTER	No	The number of HPC calls that were successfully placed on HPC CQ queues.
CQ_Q_OVERFLOWES	COUNTER	No	The number of HPC calls for which HPC CQ queuing attempts were unsuccessful because queues were full.

Column Name	Column Type	Index	Description
CQ_Q_ABANDONS	COUNTER	No	The number of HPC calls that were placed in HPC CQ queues, but were subsequently abandoned before they could be completed.
CQ_Q_TIMEOUTS	COUNTER	No	The number of HPC calls removed from HPC CQ queues due to expiration of the queue timeout timer.
EQ_Q_ATTEMPTS	COUNTER	No	The number of HPC calls that were successfully placed on HPC EQ queues.
EQ_Q_OVERFLOWS	COUNTER	No	The number of HPC calls for which HPC EQ queuing attempts were unsuccessful because the queue was full.
EQ_Q_ABANDONS	COUNTER	No	The number of HPC calls that were placed in the HPC EQ queue, but were subsequently abandoned before they could be completed.
EQ_Q_TIMEOUTS	COUNTER	No	The number of HPC calls removed from the HPC EQ queue due to expiration of the queue timeout timer.
IQ_IN_Q_ATTEMPTS	COUNTER	No	The number of HPC calls that were successfully placed on internal HPC IP Queuing queues.
IQ_IN_Q_OVERFLOWS	COUNTER	No	The number of HPC calls for which HPC IP Queuing internal queuing attempts were unsuccessful because the queue was full.
IQ_IN_Q_ABANDONS	COUNTER	No	The number of HPC calls that were placed in internal HPC IP Queuing queues, but were subsequently abandoned before it could be completed.
IQ_IN_Q_TIMEOUTS	COUNTER	No	The number of HPC calls removed from internal HPC IP Queuing queues due to expiration of the queue timeout timer.
IQ_IN_OVERSUBSCRIBE_ATTEMPTS	COUNTER	No	The number of HPC calls that encountered internal IPTGs that are over their normal resource allocations.

Column Name	Column Type	Index	Description
IQ_IN_OVERSUBSCRIBE D_CALLS	COUNTER	No	The number of HPC calls connected on internal IPTGs that are over their normal resource allocations.
IQ_EX_Q_ATTEMPTS	COUNTER	No	The number of HPC calls that were successfully placed on external HPC IP Queuing queues.
IQ_EX_Q_OVERFLOWES	COUNTER	No	The number of HPC calls for which HPC IP Queuing external queuing attempts were unsuccessful because the queue was full.
IQ_EX_Q_ABANDONS	COUNTER	No	The number of HPC calls that were placed in external HPC IP Queuing queues, but were subsequently abandoned before it could be completed.
IQ_EX_Q_TIMEOUTS	COUNTER	No	The number of HPC calls removed from external HPC IP Queuing queues due to expiration of the queue timeout timer.
IQ_EX_OVERSUBSCRIBE _ATTEMPTS	COUNTER	No	The number of HPC calls that encountered external IPTGs that are over their normal resource allocations.
IQ_EX_OVERSUBSCRIBE D_CALLS	COUNTER	No	The number of HPC calls connected on external IPTGs that are over their normal resource allocations.
TRAFFIC_CONTROL_EXE MPTIONS	COUNTER	No	The number of HPC calls that were exempted from traffic controls.
IPTG_OVERSUBSCRIPTI ONS	COUNTER	No	The number of HPC calls that were placed on IPTGs over their normal resource allocations.

GSXImStatusStats

Column Name	Column Type	Index	Description
IMSTATUSINDEX	INTEGER	Yes	A unique value for each intercept manager entry between 1 and maximum allowed.

Column Name	Column Type	Index	Description
PRI_OPER_STATE	INTEGER	No	Current operational state of the Primary Call Data Channel.
SEC_OPER_STATE	INTEGER	No	Current operational state of the Secondary Call Data Channel.
SIGNAL_START_SUCCES S	COUNTER	No	The number of successful Signal Start messages sent on the active call data channel.
SIGNAL_START_UNSUCC ESS	COUNTER	No	The number of unsuccessful Signal Start messages sent on the active call data channel.
CALL_ANSWER_SUCCES S	COUNTER	No	The number of successful Call Answer messages sent on the active call data channel.
CALL_ANSWER_UNSUCC ESS	COUNTER	No	The number of unsuccessful Call Answer messages sent on the active call data channel.
CALL_DISCONNECT_SUC CESS	COUNTER	No	The number of successful Call Disconnect messages sent on the active call data channel.
CALL_DISCONNECT_UN SUCCESS	COUNTER	No	The number of unsuccessful Call Disconnect messages sent on the active call data channel.
MEDIA_REPORT_SUCCES S	COUNTER	No	The number of successful Media Report messages sent on the active call data channel.
MEDIA_REPORT_UNSUCC CESS	COUNTER	No	The number of unsuccessful Media Report messages sent on the active call data channel.
SERVICE_INSTANCE_SUC CESS	COUNTER	No	The number of successful Service Instance messages sent on the active call data channel.
SERVICE_INSTANCE_UN SUCCESS	COUNTER	No	The number of unsuccessful Service Instance messages sent on the active call data channel.

Column Name	Column Type	Index	Description
SIGNAL_INSTANCE_SUCCESS	COUNTER	No	The number of successful Signal Instance messages sent on the active call data channel.
SIGNAL_INSTANCE_UNSUCCESS	COUNTER	No	The number of unsuccessful Signal Instance messages sent on the active call data channel.
INDICATION_SUCCESS	COUNTER	No	The number of successful Indication messages sent on the active call data channel.
INDICATION_UNSUCCESS	COUNTER	No	The number of unsuccessful Indication messages sent on the active call data channel.
KEEP_ALIVE_SUCCESS	COUNTER	No	The number of successful Keep Alive messages sent on the active call data channel.
KEEP_ALIVE_UNSUCCESS	COUNTER	No	The number of unsuccessful Keep Alive messages sent on the active call data channel.
RESTART_SUCCESS	COUNTER	No	The number of successful Restart messages sent on the active call data channel.
RESTART_UNSUCCESS	COUNTER	No	The number of unsuccessful Restart messages sent on the active call data channel.
RADIUS_ACK_RECEIVED	COUNTER	No	The number of Radius Acknowledgement messages received on the active call data channel.
RADIUS_UNKNOWN_MSG_RECEIVED	COUNTER	No	The number of messages received with an unknown Radius message code on the active call data channel.
SIGNAL_START_RESPONSE_RECEIVED	COUNTER	No	The number of Signaling Start Response messages received on the active call data channel.

Column Name	Column Type	Index	Description
SIGNAL_STOP_SUCCESS	COUNTER	No	The number of successful Signal Stop messages sent on the active call data channel.
SIGNAL_STOP_UNSUCCESS	COUNTER	No	The number of unsuccessful Signal Stop messages sent on the active call data channel.

GSXMlppIntervalStats

Column Name	Column Type	Index	Description
EGRESS_PSTN_TG_PREEMPTED_CALLS	GAUGE	No	Number of preempted calls on all Egress PSTN Trunks for the specified interval.
EGRESS_IP_TG_PREEMPTED_CALLS	GAUGE	No	Number of preempted calls on all Egress IP Trunks for the specified interval.
INGRESS_IP_TG_PREEMPTED_CALLS	GAUGE	No	Number of preempted calls on all Ingress IP Trunks for the specified interval.
EGRESS_PSTN_TG_PRE_CALLS_BLKD	GAUGE	No	Number of precedence calls blocked on all Egress PSTN Trunks for the specified interval.
EGRESS_IP_TG_PRE_CALLS_BLKD	GAUGE	No	Number of precedence calls blocked on all Egress IP Trunks for the specified interval.
INGRESS_IP_TG_PRE_CALLS_BLKD	GAUGE	No	Number of precedence calls blocked on all Ingress IP Trunks for the specified interval.
PRECD_CALLS_EXMPT_TRF_CTRL	GAUGE	No	Number of precedence calls exempt from traffic controls on all trunks for the specified interval.

GSXPeakCallStat

Column Name	Column Type	Index	Description
PEAK_PSTN_TO_SIP_CALLS	INTEGER	No	Interval Peak Count for PSTN to SIP
PEAK_PSTN_TO_H323_CALLS	INTEGER	No	Interval Peak Count for PSTN to H323
PEAK_PSTN_TO_PSTN_CALLS	INTEGER	No	Interval Peak Count for PSTN to PSTN
PEAK_PSTN_TO_SIPT_CALLS	INTEGER	No	Interval Peak Count for PSTN to SIPT
PEAK_PSTN_TO_GW_CALLS	INTEGER	No	Interval Peak Count for PSTN to GW
PEAK_SIP_TO_SIP_CALLS	INTEGER	No	Interval Peak Count for SIP to SIP
PEAK_SIP_TO_GW_CALLS	INTEGER	No	Interval Peak Count for SIP to GW
PEAK_SIP_TO_H323_CALLS	INTEGER	No	Interval Peak Count for SIP to H323
PEAK_H323_TO_H323_CALLS	INTEGER	No	Interval Peak Count for H323 to H323
PEAK_H323_TO_GW_CALLS	INTEGER	No	Interval Peak Count for H323 to GW
PEAK_PKT_TO_PKT_CALLS	INTEGER	No	Interval Peak Count for Packet to Packet
PEAK_SIPT_TO_SIP_CALLS	INTEGER	No	Interval Peak Count for SIPT to SIP
PEAK_SIPT_TO_GW_CALLS	INTEGER	No	Interval Peak Count for SIPT to GW
PEAK_SIPT_TO_H323_CALLS	INTEGER	No	Interval Peak Count for SIPT to H323
PEAK_SIPT_TO_SIPT_CALLS	INTEGER	No	Interval Peak Count for SIPT to SIPT

GSXSipHpcIntervalStats

Column Name	Column Type	Index	Description
ETS_INVITES_OUT	COUNTER	No	Generated INVITES containing RPH with ETS.
ETS_RINGING	COUNTER	No	Generated 180 INVITE responses containing RPH with ETS.
ETS_QUEUED	COUNTER	No	Generated 182 INVITE responses containing RPH with ETS.
ETS_SUCCESS	COUNTER	No	Generated 200 INVITE responses containing RPH with ETS.
ETS_FAILURE	COUNTER	No	Generated 4xx INVITE responses containing RPH with ETS.
ETS_BAD_REQUEST_OUT	COUNTER	No	Generated 400 responses (with 417 reason) containing RPH with ETS.
ETS_TIMEOUT	COUNTER	No	Generated 408 INVITE responses containing RPH with ETS.
ETS_UNKNOWN_RP	COUNTER	No	Generated 417 INVITE responses containing RPH with ETS.
ETS_BUSY_HERE	COUNTER	No	Generated 486 INVITE responses containing RPH with ETS.
ETS_INVITES_IN	COUNTER	No	Received INVITES containing RPH with ETS.
ETS_INVITES_ETS_DN	COUNTER	No	Received INVITES with ETSDN but no RPH with ETS.
ETS_BAD_REQUEST_IN	COUNTER	No	Received 400 INVITE responses (with 417 reason) containing RPH with ETS.
ETS_UNKNOWN_RP_IN	COUNTER	No	Received 417 INVITE responses containing RPH with ETS.
ETS_BAD_EXTN_IN	COUNTER	No	Received 420 INVITE responses containing RPH with ETS.

Column Name	Column Type	Index	Description
ETS_FORBIDDEN_IN	COUNTER	No	Indicates the received 403 INVITE responses for HPC calls.
ETS_LOGS_GENERATED	COUNTER	No	Number of ETS related logs generated.
ETS_183_OUT	COUNTER	No	Generated 183 INVITE responses containing RPH with ETS.
ETS_403_OUT	COUNTER	No	Indicates the sent 403 reject responses for HPC calls.
ETS_600_OUT	COUNTER	No	Generated 600 INVITE responses containing RPH with ETS.
ETS_600_IN	COUNTER	No	Indicates the received 600 INVITE responses for HPC calls.

GSXSipHpcLimitStats

Column Name	Column Type	Index	Description
HPC_LIMIT_INDEX	INTEGER	Yes	Index of this Hpc Limit Status table entry.
STAT_NAME	STRING	No	The name of the corresponding sonusHpcLimitEntry.
INGRESS_HPC_CALLS_ALLOWED	COUNTER	No	The number of ingress HPC call attempts allowed under an HPC limit.
INGRESS_HPC_CALLS_DENIED_RATE	COUNTER	No	The number of ingress HPC call attempts denied because they exceeded the rate allowed by an HPC limit.
INGRESS_HPC_CALLS_DENIED_NUMBER	COUNTER	No	The number of ingress HPC call attempts denied because they exceeded the number of simultaneous calls allowed by an HPC limit.
CURRENT_INGRESS_HPC_CALLS	COUNTER	No	The number of active plus stable ingress HPC calls from the SIP peers subject to an HPC limit.
EGRESS_HPC_CALLS_ALLOWED	COUNTER	No	The number of egress HPC call attempts allowed under an HPC limit.

Column Name	Column Type	Index	Description
EGRESS_HPC_CALLS_DENIED_NUMBER	COUNTER	No	The number of egress HPC call attempts denied because they exceeded the number of simultaneous calls allowed by an HPC limit.
CURRENT_EGRESS_HPC_CALLS	COUNTER	No	The number of active plus stable egress HPC calls to the SIP peers subject to an HPC limit.

GSXSipSigPortTlsStats

Column Name	Column Type	Index	Description
SSP_INDEX	GAUGE	Yes	Identifies the SIP Signaling Port entry.
ACTIVE_CLIENT_SESSIONS	GAUGE	No	Number of current up sessions in which the GSX is the client.
ACTIVE_SERVER_SESSIONS	GAUGE	No	Number of current up sessions in which the GSX is the server.
SUSPENDED_CLIENT_SESSIONS	GAUGE	No	Number of current suspended sessions in which the GSX is the client.
SUSPENDED_SERVER_SESSIONS	GAUGE	No	Number of current suspended sessions in which the GSX is the server.
INC_CLIENT_HANDSHAKES	GAUGE	No	Number of current incomplete handshakes in which the GSX is the client.
INC_SERVER_HANDSHAKES	GAUGE	No	Number of current incomplete handshakes in which the GSX is the server.
TOTAL_CLIENT_SESSIONS	COUNTER	No	Cumulative total number of sessions in which the GSX is the client.
TOTAL_SERVER_SESSIONS	COUNTER	No	Cumulative total number of sessions in which the GSX is the server.
TOTAL_SERVER_RESUMED	COUNTER	No	Number of sessions that have been resumed in which the GSX is the server.
NO_CIPHER_SUITE	COUNTER	No	Number of handshake failures due to inability to converge on a cipher suite.

Column Name	Column Type	Index	Description
HANDSHAKE_TIMEOUT	COUNTER	No	Number of handshakes that timed out before completing.
HIGHER_AUTH_TIMEOUT	COUNTER	No	The number of client handshakes with the GSX when the client did not authenticate itself through TLS and failed to authenticate itself through any higher level protocol (for example, SIP) before timing out
CLIENT_AUTH_FAIL	COUNTER	No	Number of times peer failed TLS authentication when the GSX was the client.
SERVER_AUTH_FAIL	COUNTER	No	Number of times peer failed TLS authentication when the GSX was the server.
FATAL_ALERTS	COUNTER	No	Number of FATAL Alerts received.
WARNING_ALERTS	COUNTER	No	Number of WARNING Alerts received.
HANDSHAKE_FAILS	COUNTER	No	Cumulative total of all handshake failures.
RCV_FAILS	COUNTER	No	Number of receive failures (failure to decrypt).
SEND_FAILS	COUNTER	No	Number of send failures (failure to encrypt)
NO_AUTH_DROPS	COUNTER	No	Number of SIP messages dropped due to lack of peer authentication at the SIP level.
NO_AUTH488	COUNTER	No	Number of SIP messages rejected with 488 due to lack of peer authentication at the SIP level.
MID_CONN_HELLO	COUNTER	No	Number of times a peer sent a TLS Hello on a connection that was already up (that is, the peer tried to renegotiate.)
NO_CLIENT_CERT	COUNTER	No	Number of times we were the client and we failed to derive a certificate to send the server (in the mutual authentication case). This is probably because there was no overlap between our configured trust anchors and the list of trust anchors the server sent in its Certificate Request

Column Name	Column Type	Index	Description
COUNT_RESET	INTEGER	No	Set operation on this object resets all the TLS statistics counts to zero.

GSXSipSigPortTlsStatusStats

Column Name	Column Type	Index	Description
SSPINDEX	GAUGE	Yes	Identifies the SIP Signaling Port entry.
PEER_IP_ADDRESS	IPADDRESS	Yes	Identifies the IP Address of the peer of this session.
TLS_SESSION	GAUGE	Yes	Identifies the TLS session. This is an internal session tracking number and should not be confused with the session ID that is actually used on the wire between the TLS peers.
PEER_PORT_NUM	INTEGER	No	Identifies the TCP Port number used by the peer of this session.
SOCKET	INTEGER	No	Identifies the socket number used internally for the TCP component of this session.
TLS_SESSION_ID	OCTETSTRING	No	The TLS Session ID of this session.
CONN_ID	INTEGER	No	The current internal connection ID of this session (0 means none, that is, suspended session)
SESS_STATE	INTEGER	No	The connection state of this session.
ROLE	INTEGER	No	The role taken by the GSX in this session.
RESUMPTIONS	COUNTER	No	The number of times this session has been resumed.
BYTES_SENT	COUNTER	No	The number of payload bytes sent on the current connection associated with this session.
RECORDS_SENT	COUNTER	No	The number of TLS records sent on the current connection associated with this session.

Column Name	Column Type	Index	Description
BYTES_REC_OK	COUNTER	No	The number of payload bytes received on the current connection without an integrity check failure.
RECORDS_REC_OK	COUNTER	No	The number of TLS records received on the current connection without an integrity check failure.
ROW_STATUS	INTEGER	No	This is for SNMP use.
PEER_IPV6_ADDRESSES	IPV6ADDRESS	Yes	Identifies IPv6 address of the peer of this session.
PEER_IPVERSION	INTEGER	Yes	The role taken by the GSX in this session.

GSXSlotDspResIntervalStats

Column Name	Column Type	Index	Description
SLOT_INDEX	INTEGER	Yes	Identifies the target card.
G711CIRCUIT_PEAK_USED	GAUGE	No	The peak usage of type G711 Circuit DSP pad during an interval time.
G711CIRCUIT_AVERAGE_USED	GAUGE	No	The average usage of type G711 Circuit DSP pad during an interval time.
G711CIRCUIT_AVERAGE_AVAIL	GAUGE	No	The average availability of type G711 Circuit DSP pad during an interval time.
TONE_PEAK_USED	GAUGE	No	The Interval number of Peak usage of type Tone DSP pad during an interval time.
TONE_AVERAGE_USED	GAUGE	No	The average usage of type Tone DSP pad during an interval time.
TONE_AVERAGE_AVAIL	GAUGE	No	The average availability of type Tone DSP pad during an interval time.
BRIDGEPORT_PEAK_USED	GAUGE	No	The peak usage of type Bridge Port DSP pad during an interval time.

Column Name	Column Type	Index	Description
BRIDGEPORT_AVERAGE_USED	GAUGE	No	The average usage of type Bridge Port DSP pad during an interval time.
BRIDGEPORT_AVERAGE_AVAIL	GAUGE	No	The average availability of type Bridge Port DSP pad during an interval time.
G729_PEAK_USED	GAUGE	No	The peak usage of type G729 DSP pad during an interval time.
G729_AVERAGE_USED	GAUGE	No	The average usage of type G729 DSP pad during an interval time.
G729_AVERAGE_AVAIL	GAUGE	No	The average availability of type G729 DSP pad during an interval time.
G726_PEAK_USED	GAUGE	No	The Interval number of Peak usage of type G726 DSP pad during an interval time.
G726_AVERAGE_USED	GAUGE	No	The average usage of type G726 DSP pad during an interval time.
G726_AVERAGE_AVAIL	GAUGE	No	The average availability of type G726 DSP pad during an interval time.
G723_PEAK_USED	GAUGE	No	The peak usage of type G723 DSP pad during an interval time.
G723_AVERAGE_USED	GAUGE	No	The average usage of type G723 DSP pad during an interval time.
G723_AVERAGE_AVAIL	GAUGE	No	The average availability of type G723 DSP pad during an interval time.
G711PACKET_PEAK_USED	GAUGE	No	The peak usage of type G711 Packet DSP pad during an interval time.
G711PACKET_AVERAGE_USED	GAUGE	No	The average usage of type G711 Packet DSP pad during an interval time.
G711PACKET_AVERAGE_AVAIL	GAUGE	No	The average availability of type G711 Packet DSP pad during an interval time.

Column Name	Column Type	Index	Description
T38_PEAK_USED	GAUGE	No	The peak usage of type T38 DSP pad during an interval time.
T38_AVERAGE_USED	GAUGE	No	The average usage of type T38 DSP pad during an interval time.
T38_AVERAGE_AVAIL	GAUGE	No	The average availability of type T38 DSP pad during an interval time.
EVRC_PEAK_USED	GAUGE	No	The peak usage of type EVRC DSP pad during an interval time.
EVRC_AVERAGE_USED	GAUGE	No	The average usage of type EVRC DSP pad during an interval time.
EVRC_AVERAGE_AVAIL	GAUGE	No	The average availability of type EVRC DSP pad during an interval time.
GSM_PEAK_USED	GAUGE	No	The peak usage of type GSM DSP pad during an interval time.
GSM_AVERAGE_USED	GAUGE	No	The average usage of type GSM DSP pad during an interval time.
GSM_AVERAGE_AVAIL	GAUGE	No	The average availability of type GSM DSP pad during an interval time.
T38_ECM_PEAK_USED	GAUGE	No	The peak usage of type T38 ECM capable DSP pad during an interval time.
T38_ECM_AVERAGE_USED	GAUGE	No	The average usage of type T38 ECM capable DSP pad during an interval time.
T38_ECM_AVERAGE_AVAIL	GAUGE	No	The average availability of type T38 ECM capable DSP pad during an interval time.
EVRCB0_PEAK_USED	GAUGE	No	The peak usage of type EVRCB0 DSP pad during an interval time.
EVRCB0_AVERAGE_USED	GAUGE	No	The average usage of type EVRCB0 DSP pad during an interval time.

Column Name	Column Type	Index	Description
EVRCB0_AVERAGE_AVAIL	GAUGE	No	The average availability of type EVRCB0 DSP pad during an interval time.
INTERVAL_LBCPEAK_USED	GAUGE	No	The peak usage of type iLBC DSP pad during an interval time.
INTERVAL_LBCAVERAGE_USED	GAUGE	No	The average usage of type iLBC DSP pad during an interval time.
INTERVAL_LBCAVERAGE_AVAIL	GAUGE	No	The average availability of type iLBC DSP pad during an interval time.
G722_PEAK_USED	GAUGE	No	The peak usage of type G722 DSP pad during an interval time.
G722_AVERAGE_USED	GAUGE	No	The average usage of type G722 DSP pad during an interval time.
G722_AVERAGE_AVAIL	GAUGE	No	The average availability of type G722 DSP pad during an interval time.
AMRWB_PEAK_USED	GAUGE	No	The peak usage of type AMRWB DSP pad during an interval time.
AMRWB_AVERAGE_USED	GAUGE	No	The average usage of type AMRWB DSP pad during an interval time.
AMRWB_AVERAGE_AVAIL	GAUGE	No	The average availability of type AMRWB DSP pad during an interval time.

Note

File based collection (SFTP) includes slots that are enabled and ACTIVE.
 SNMP collection includes slots that are enabled irrespective of the status (ACTIVE or STANDBY).

GSXSonicBusUsageIntervalStats

Column Name	Column Type	Index	Description
INTERVAL_SONIC_BUS_USAGE	GAUGE	No	Current sonic Bus usage in the midplane.

Column Name	Column Type	Index	Description
INTERVAL_SONIC_BUS_PEAK_USAGE	GAUGE	No	SonicBus Usage in the midplane for the specified interval.
INTERVAL_SONIC_BUS_AVG_USAGE	GAUGE	No	SonicBus Usage in the midplane for the specified interval.

Ss7DestinationStats

Column Name	Column Type	Index	Description
SS7_DESTINATION_INDEX	INTEGER	Yes	The index of the SS7 destination status entry.
SS7_DESTINATION_STATE	INTEGER	False	The current state of the specified SS7 destination.
SS7_DESTINATION_CONGESTION_LEVEL	INTEGER	False	The congestion level of the SS7 destination.
SS7_DEST_DISCARD_LEVEL	INTEGER	False	The discard level of the SS7 destination.
SS7_DEST_MSU_DISCARDING	INTEGER	False	The number of MSUs that have been discarded over the measured interval as a result of routing error -- a Q.752 statistics item.
SS7_DEST_MSU_DISCONGESTION	INTEGER	False	The number of MSUs that have been discarded over the measured interval as a result of destination congestion -- a Q.752 statistics item.
SS7_DEST_INACCESSIBLE_TIMES	INTEGER	False	The number of times that the destination has become inaccessible over the measured interval -- a Q.752 statistics.
SS7_DEST_INACCESSIBLE_START_TIME	INTEGER	False	The start time at which the destination became inaccessible -- a Q.752 statistics item.
SS7_DEST_INACCESSIBLE_STOP_TIME	INTEGER	False	The stop time at which the destination became inaccessible -- a Q.752 statistics item.

Column Name	Column Type	Index	Description
SS7_DEST_INACC_DURATION	INTEGER	False	The duration during which the destination remained inaccessible -- a Q.752 statistics item.
SS7_DESTINATION_NAME	STRING	False	The name of this SS7 Destination instance.
SS7_DESTINATION_TYPE	INTEGER	False	Type of the destination, such as an adjacent node, a remote node, or a (remote) cluster.

Ss7LinkStats

Column Name	Column Type	Index	Description
SS7_LINK_INDEX	INTEGER	Yes	The index of the SS7 link.
SS7_LINK_STATE	OCTETSTRING	No	The current state of the SS7 link.
SS7_LINK_RECEIVED_SIO	INTEGER	No	The number of SIOs received on this link over the measured interval -- a Q.752 statistics item.
SS7_LINK_RECEIVED_SIF	INTEGER	No	The number of SIF bytes received on this link over the measured interval -- a Q.752 statistics item.
SS7_LINK_TRANSMITTED_SIO	INTEGER	No	The number of SIOs transmitted on this link over the measured interval -- a Q.752 statistics item.
SS7_LINK_TRANSMITTED_SIF	INTEGER	No	The number of SIF bytes transmitted on this link over the measured interval -- a Q.752 statistics item.
LINK_UNAVL_START_TIME	INTEGER	No	The start time at which the link became unavailable -- a Q.752 statistics item.
LINK_UNAVL_STOP_TIME	INTEGER	No	The stop time at which the link became unavailable -- a Q.752 statistics item.
LINK_UNAVL_DURATION	INTEGER	No	The duration during which the link remained unavailable -- a Q.752 statistics item.

Column Name	Column Type	Index	Description
LINK_ACTIVATION_STATUS	INTEGER	No	The current activation/deactivation status of the link.
LINK_PERIODIC_SLT_STATUS	INTEGER	No	The current periodic SLT status of the link.
LINK_CONGESTION_LEVEL	INTEGER	No	The current congestion level of the link.
LINK_DISCARD_LEVEL	INTEGER	No	The current discard level of the link.
LINK_RESTITUTION_ATTEMPTS	INTEGER	No	The successive restoration attempts the link has performed since the link became unavailable.
LINK_SLT_TESTS	INTEGER	No	The successive SLTM/SLTA tests the link has been performed.
SS7_LINK_NAME	INTEGER	No	The Name of the SS7 link.
SS7_LINK_TYPE	INTEGER	No	The Type of the SS7 link.
INGRESS_LINK_UTILIZATION	INTEGER	No	Shows the Ingress Utilisation of a SS7 Link.
EGRESS_LINK_UTILIZATION	INTEGER	No	Shows the Egress Utilisation of a SS7 Link.

Ss7RouteStats

Column Name	Column Type	Index	Description
ROUTE_STATUS_INDEX	INTEGER	Yes	The index of the SS7 route status
SS7_ROUTE_STATE	OCTETSTRING	No	The current state of the SS7 route
ROUTE_CONGESTION_LEVEL	INTEGER	No	The current congestion level of the route
SS7_ROUTE_NAME	STRING	No	The name of the SS7 route
SS7_ROUTE_TYPE	INTEGER	No	The type of the SS7 route

GSXSysCallDspResIntervalStats

Column Name	Column Type	Index	Description
SUCCESS_NO_DSP_ALLO C_FAILURE	COUNTER	No	The number of successful calls during the interval without DSP resource allocation failure.
SUCCESS_WITH_DSP_AL LOC_FAILURE	COUNTER	No	The number of successful calls during the interval with DSP resource allocation failure.
FAIL_NO_G711CIRCUIT	COUNTER	No	The number of calls failed due to lack of G711 Circuit DSP resource during the interval time.
FAIL_OTHER_ON_G711CI RCUIT	COUNTER	No	The number of calls failed due to reason other than lack G711 Circuit DSP resource during the interval time.
SUCCESS_NO_G711CIRC UIT	COUNTER	No	The number of successful calls even with a lack of G711 Circuit DSP resources during a interval time.
FAIL_NO_TONE	COUNTER	No	The number of calls failed due to lack of Tone DSP resource during the interval time.
FAIL_OTHER_ON_TONE	COUNTER	No	The number of calls failed due to reason other than lack Tone DSP resource during the interval time.
SUCCESS_NO_TONE	COUNTER	No	The number of successful calls even with a lack of Tone DSP resources during a interval time.
FAIL_NO_BRIDGEPORT	COUNTER	No	The number of calls failed due to lack of Bridge Port DSP resource during the interval time.
FAIL_OTHER_ON_BRIDGE PORT	COUNTER	No	The number of calls failed due to reason other than lack Bridge Port DSP resource during the interval time.
SUCCESS_NO_BRIDGEP ORT	COUNTER	No	The number of successful calls even with a lack of Bridge Port DSP resources during a interval time.

Column Name	Column Type	Index	Description
FAIL_NO_G729	COUNTER	No	The number of calls failed due to lack of G729 DSP resource during the interval time.
FAIL_OTHER_ON_G729	COUNTER	No	The number of calls failed due to reason other than lack G729 DSP resource during the interval time.
SUCCESS_NO_G729	COUNTER	No	The number of successful calls even with a lack of G729 DSP resources during a interval time.
FAIL_NO_G726	COUNTER	No	The number of calls failed due to lack of G726 DSP resource during the interval time.
FAIL_OTHER_ON_G726	COUNTER	No	The number of calls failed due to reason other than lack G726 DSP resource during the interval time.
SUCCESS_NO_G726	COUNTER	No	The number of successful calls even with a lack of G726 DSP resources during a interval time.
FAIL_NO_G723	COUNTER	No	The number of calls failed due to lack of G723 DSP resource during the interval time.
FAIL_OTHER_ON_G723	COUNTER	No	The number of calls failed due to reason other than lack G723 DSP resource during the interval time.
SUCCESS_NO_G723	COUNTER	No	The number of successful calls even with a lack of G723 DSP resources during a interval time.
FAIL_NO_G711PACKET	COUNTER	No	The number of calls failed due to lack of G711 Packet DSP resource during the interval time.
FAIL_OTHER_ON_G711PACKET	COUNTER	No	The number of calls failed due to reason other than lack G711 Packet DSP resource during the interval time.

Column Name	Column Type	Index	Description
SUCCESS_NO_G711PACKET	COUNTER	No	The number of successful calls even with a lack of G711 Packet DSP resources during a interval time.
FAIL_NO_T38	COUNTER	No	The number of calls failed due to lack of T38 DSP resource during the interval time.
FAIL_OTHER_ON_T38	COUNTER	No	The number of calls failed due to reason other than lack T38 DSP resource during the interval time.
SUCCESS_NO_T38	COUNTER	No	The number of successful calls even with a lack of T38 DSP resources during a interval time.
FAIL_NO_EVRC	GAUGE	No	The number of calls failed due to lack of EVRC DSP resource during the interval time.
FAIL_OTHER_ON_EVRC	GAUGE	No	The number of call fails due to reason other than lack EVRC DSP resource during a interval time.
SUCCESS_NO_EVRC	GAUGE	No	The number of call was successful even though lack of EVRC DSP resource during a interval time.
FAIL_NO_GSM	GAUGE	No	The number of call failed due to lack of GSM DSP resource during a interval time.
FAIL_OTHER_ON_GSM	GAUGE	No	The number of call fails due to reason other than lack GSM DSP resource during a interval time.
SUCCESS_NO_GSM	GAUGE	No	The number of call was successful even though lack of GSM DSP resource during a interval time.
FAIL_NO_T38_ECM	GAUGE	No	The number of call failed due to lack of T38 ECM capable DSP resource during a interval time.

Column Name	Column Type	Index	Description
FAIL_OTHER_ON_T38_ECM	GAUGE	No	The number of call fails due to reason other than lack T38 ECM capable DSP resource during a interval time.
SUCCESS_NO_T38_ECM	GAUGE	No	The number of call was successful even though lack of T38 ECM capable DSP resource during a interval time.
FAIL_NO_G722	GAUGE	No	The number of call failed due to lack of G722 DSP resource during a interval time.
FAIL_OTHER_ON_G722	GAUGE	No	The number of call fails due to reason other than lack G722 DSP resource during a interval time.
SUCCESS_NO_G722	GAUGE	No	The number of call was successful even though lack of G722 DSP resource during a interval time.
FAIL_NO_AMRWB	GAUGE	No	The number of call failed due to lack of AMRWB DSP resource during a interval time.
FAIL_OTHER_ON_AMRWB	GAUGE	No	The number of call fails due to reason other than lack AMRWB DSP resource during a interval time.
SUCCESS_NO_AMRWB	GAUGE	No	The number of call was successful even though lack of AMRWB DSP resource during a interval time.

GSXSysDspResHighestUsageStats

GSXSysDspResHighestUsageStats table stores the highest percent of PAD resource used during a one hour period on a per resource pool basis.

The Highest Used Percent is calculated (for each resource pool type) as:

$$(TOTAL\_PEAK\_USED / (TOTAL\_AVERAGE\_USED + TOTAL\_AVERAGE\_AVAIL)) * 100$$

The system calculates the values using the data from the preceding complete hour of data and rounds the values to the nearest integer. For example, if the collection interval is 5 minutes, a new set of rows are written to this table every 5 minutes, with the totals calculated by taking into account the last 12 collections. If the collection interval is 15 minutes, the totals used are from the last 4 collections.

Column Name	Column Type	Index	Description
CONTRIBUTORS	INTEGER	No	The number of rows used in the calculation of the percentage. For 5-minute intervals, it is "12"; for 15-minute intervals, it is "4".
G711CIRCUIT_PERCENT_USAGE	INTEGER	No	The highest percent usage for G711 Circuit resource.
TONE_PERCENT_USAGE	INTEGER	No	The highest percent usage for Tone resource.
BRIDGEPORT_PERCENT_USAGE	INTEGER	No	The highest percent usage for Bridge Port resource.
G729_PERCENT_USAGE	INTEGER	No	The highest percent usage for G729 resource.
G726_PERCENT_USAGE	INTEGER	No	The highest percent usage for G726 resource.
G723_PERCENT_USAGE	INTEGER	No	The highest percent usage for G723 resource.
G711PACKET_PERCENT_USAGE	INTEGER	No	The highest percent usage for G711 Packet resource.
T38_PERCENT_USAGE	INTEGER	No	The highest percent usage for T38 resource.

GSXSysDspResIntervalStats

Column Name	Column Type	Index	Description
G711CIRCUIT_PEAK_USED	GAUGE	No	The peak usage of type G711 Circuit DSP pad during an interval time.
G711CIRCUIT_AVERAGE_USED	GAUGE	No	The average usage of type G711 Circuit DSP pad during an interval time.
G711CIRCUIT_AVERAGE_AVAIL	GAUGE	No	The average availability of type G711 Circuit DSP pad during an interval time.
TONE_PEAK_USED	GAUGE	No	The peak usage of type Tone DSP pad during an interval time.

Column Name	Column Type	Index	Description
TONE_AVERAGE_USED	GAUGE	No	The average usage of type Tone DSP pad during an interval time.
TONE_AVERAGE_AVAIL	GAUGE	No	The average availability of type Tone DSP pad during an interval time.
BRIDGEPORT_PEAK_USED	GAUGE	No	The peak usage of type Bridge Port DSP pad during an interval time.
BRIDGEPORT_AVERAGE_USED	GAUGE	No	The average usage of type Bridge Port DSP pad during an interval time.
BRIDGEPORT_AVERAGE_AVAIL	GAUGE	No	The average availability of type Bridge Port DSP pad during an interval time.
G729_PEAK_USED	GAUGE	No	The peak usage of type G729 DSP pad during an interval time.
G729_AVERAGE_USED	GAUGE	No	The average usage of type G729 DSP pad during an interval time.
G729_AVERAGE_AVAIL	GAUGE	No	The average availability of type G729 DSP pad during an interval time.
G726_PEAK_USED	GAUGE	No	The peak usage of type G726 DSP pad during an interval time.
G726_AVERAGE_USED	GAUGE	No	The average usage of type G726 DSP pad during an interval time.
G726_AVERAGE_AVAIL	GAUGE	No	The average availability of type G726 DSP pad during an interval time.
G723_PEAK_USED	GAUGE	No	The peak usage of type G723 DSP pad during an interval time.
G723_AVERAGE_USED	GAUGE	No	The average usage of type G723 DSP pad during an interval time.
G723_AVERAGE_AVAIL	GAUGE	No	The average availability of type G723 DSP pad during an interval time.
G711PACKET_PEAK_USED	GAUGE	No	The peak usage of type G711 Packet DSP pad during an interval time.

Column Name	Column Type	Index	Description
G711PACKET_AVERAGE_USED	GAUGE	No	The average usage of type G711 Packet DSP pad during an interval time.
G711PACKET_AVERAGE_AVAIL	GAUGE	No	The average availability of type G711 Packet DSP pad during an interval time.
T38_PEAK_USED	GAUGE	No	The peak usage of type T38 DSP pad during an interval time.
T38_AVERAGE_USED	GAUGE	No	The average usage of type T38 DSP pad during an interval time.
T38_AVERAGE_AVAIL	GAUGE	No	The average availability of type T38 DSP pad during an interval time.
EVRC_PEAK_USED	GAUGE	No	The peak usage of type EVRC DSP pad during an interval time.
EVRC_AVERAGE_USED	GAUGE	No	The average usage of type EVRC DSP pad during an interval time.
EVRC_AVERAGE_AVAIL	GAUGE	No	The average availability of type EVRC DSP pad during an interval time.
GSM_PEAK_USED	GAUGE	No	The peak usage of type GSM DSP pad during an interval time.
GSM_AVERAGE_USED	GAUGE	No	The average usage of type GSM DSP pad during an interval time.
GSM_AVERAGE_AVAIL	GAUGE	No	The average availability of type GSM DSP pad during an interval time.
T38_ECM_PEAK_USED	GAUGE	No	The peak usage of type T38 ECM capable DSP pad during an interval time.
T38_ECM_AVERAGE_USED	GAUGE	No	The average usage of type T38 ECM capable DSP pad during an interval time.

Column Name	Column Type	Index	Description
T38_ECM_AVERAGE_AVAIL	GAUGE	No	The average availability of type T38 ECM capable DSP pad during an interval time.
EVRCB0_PEAK_USED	GAUGE	No	The peak usage of type EVRCB0 DSP pad during an interval time.
EVRCB0_AVERAGE_USED	GAUGE	No	The average usage of type EVRCB0 DSP pad during an interval time.
EVRCB0_AVERAGE_AVAIL	GAUGE	No	The average availability of type EVRCB0 DSP pad during an interval time.
INTERVALI_LBCPEAK_USED	GAUGE	No	The peak usage of type iLBC DSP pad during an interval time.
INTERVALI_LBCAVERAGE_USED	GAUGE	No	The average usage of type iLBC DSP pad during an interval time.
INTERVALI_LBCAVERAGE_AVAIL	GAUGE	No	The average availability of type iLBC DSP pad during an interval time.
G722_PEAK_USED	GAUGE	No	The peak usage of type G722 DSP pad during an interval time.
G722_AVERAGE_USED	GAUGE	No	The average usage of type G722 DSP pad during an interval time.
G722_AVERAGE_AVAIL	GAUGE	No	The average availability of type G722 DSP pad during an interval time.
AMRWB_PEAK_USED	GAUGE	No	The peak usage of type Amrwb DSP pad during an interval time.
AMRWB_AVERAGE_USED	GAUGE	No	The average usage of type Amrwb DSP pad during an interval time.
AMRWB_AVERAGE_AVAIL	GAUGE	No	The average availability of type Amrwb DSP pad during an interval time.

GsxTgIntervalStats

Note

GSXTgIntervalStats table contains the aggregate data for all trunk groups on a GSX per truck group interval. For example, if there are 4 distinct intervals 5 minutes apart and there are 10 trunk groups on the GSX, then there are 4 rows in the GsxTgIntervalStats table, with each row being the aggregate of column values for all the trunk groups for that time interval.

Column Name	Column Type	Index	Description
TG_IN_USAGE	COUNTER	No	The number of usage seconds for incoming actual call traffic on a 2way trunk group.
TG_OUT_USAGE	COUNTER	No	The number of usage seconds for outgoing actual call traffic on a 2way trunk group.
TOTAL_USAGE_SECS	INTEGER	No	The number of usage seconds for actual call traffic in both directions on a trunk group.
TG_IN_CALLS	COUNTER	No	The number of incoming calls on a trunk group that were answered.
TG_OUT_CALLS	COUNTER	No	The number of outgoing calls on a trunk group that were answered.
TG_IN_CALL_ATTEMPTS	COUNTER	No	The number of incoming seizures on a trunk group, including seizures that subsequently fail or are abandoned before routing.
TG_OUT_CALL_ATTEMPTS	COUNTER	No	The number of outgoing calls on a trunk group that successfully seized a trunk.
TG_MAX_COMPLETED_CALLS	INTEGER	No	The maximum number of completed calls in the inbound and outbound direction for this trunk group for the specified interval.
TG_TOTAL_CALL_SETUP_TIME	COUNTER	No	The total call setup time for all completed calls in the inbound and outbound directions for this trunk group for the specified interval measured in hundredths of a second. Use this object as the numerator for calculating average call setup time

Column Name	Column Type	Index	Description
TG_CALL_SETUPS	COUNTER	No	The total number of calls setup but not necessarily completed in the inbound and outbound directions for this trunk group for the specified interval. Use this object as the numerator for calculating average call setup time.
TG_IN_CALL_FAIL_NO_ROUTES	COUNTER	No	The number of inbound failed calls because there was no route available for this trunk group for the specified interval.
TG_IN_CALL_FAIL_NO_RESOURCES	COUNTER	No	The number of inbound failed calls because there was an unavailable resource for this trunk group for the specified interval.
TG_IN_CALL_FAIL_NO_SERVICE	COUNTER	No	The number of inbound failed calls because there was an unavailable service for this trunk group for the specified interval.
TG_IN_CALL_FAIL_INVALID_CALL	COUNTER	No	The number of inbound failed calls because there was an invalid call attempt for this trunk group for the specified interval.
TG_IN_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	The number of inbound failed calls because there was a network failure for this trunk group for the specified interval.
TG_IN_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	The number of inbound failed calls because there was a protocol error for this trunk group for the specified interval.
TG_IN_CALL_FAIL_UNSPECIFIED	COUNTER	No	The number of inbound failed calls for an unspecified reason for this trunk group for the specified interval.
TG_OUT_CALL_FAIL_NO_ROUTES	COUNTER	No	The number of outbound failed calls because there was no route available for this trunk group for the specified interval.
TG_OUT_CALL_FAIL_NO_RESOURCES	COUNTER	No	The number of outbound failed calls because there was an unavailable resource for this trunk group for the specified interval.
TG_OUT_CALL_FAIL_NO_SERVICE	COUNTER	No	The number of outbound failed calls because there was an unavailable service for this trunk group for the specified interval.

Column Name	Column Type	Index	Description
TG_OUT_CALL_FAIL_IN VALID_CALL	COUNTER	No	The number of outbound failed calls because there was an invalid call attempt for this trunk group for the specified interval.
TG_OUT_CALL_FAIL_N W_FAILURE	COUNTER	No	The number of outbound failed calls because there was a network failure for this trunk group for the specified interval.
TG_OUT_CALL_FAIL_PR OTOCOL_ERR	COUNTER	No	The number of outbound failed calls because there was a protocol error for this trunk group for the specified interval.
TG_OUT_CALL_FAIL_UN SPECIFIED	COUNTER	No	The number of outbound failed calls for an unspecified reason for this trunk group for the specified interval.
ROUTING_ATTEMPTS	COUNTER	No	The number of calls routed to a trunk group.
ROUTING_FAILS_NO_C KTS	COUNTER	No	The number of outgoing call attempts on a trunk group that could not be served because all circuits were in use.
ROUTING_FAILS_SFG	COUNTER	No	The current number of routing failures due to a Simulated Facilities Group for this trunk group operating at its capacity.
ROUTING_FAILS_RESV	COUNTER	No	The current number of routing failures due to no unreserved circuits available for this trunk group.
OUT_TRUNK_START_TI MEOUT	COUNTER	No	The number of outgoing trunk start timeouts for this trunk group for the specified interval.
SILC	COUNTER	No	The number of calls cancelled due to SILC for this trunk group for the specified interval.
STRCANT	COUNTER	No	The number of calls cancelled due to STR for this trunk group for the specified interval.
STRSKIP	COUNTER	No	The number of calls skipped due to STR for this trunk group for the specified interval.
SKIP	COUNTER	No	The number calls skipped due to the SKIP traffic control for this trunk group for the specified interval.

Column Name	Column Type	Index	Description
CANT	COUNTER	No	The number of calls cancelled due to CANT for this trunk group for the specified interval.
CANF	COUNTER	No	The number of calls cancelled due to CANF for this trunk group for the specified interval.
ACCCANT	COUNTER	No	The number of calls cancelled due to ACC for this trunk group for the specified interval.
ACCSKIP	COUNTER	No	The number of calls skipped due to ACC for this trunk group for the specified interval.
ROUTE_ATTEMPTS_IRR	COUNTER	No	The number of reroute attempts due to IRR for this trunk group for the specified interval.
ROUTE_ATTEMPTS_SIR R	COUNTER	No	The number of reroute attempts due to SIRR for this trunk group for the specified interval.
ROUTE_ATTEMPTS_OR R	COUNTER	No	The number of reroute attempts due to ORR for this trunk group for the specified interval.
ROUTE_ATTEMPTS_SO RR	COUNTER	No	The number of reroute attempts due to SORR for this trunk group for the specified interval.
SUCCESSFUL_IRR	COUNTER	No	The number of successful reroutes due to IRR for this trunk group for the specified interval.
SUCCESSFUL_SIRR	COUNTER	No	The number of successful reroutes due to SIRR for this trunk group for the specified interval.
SUCCESSFUL_ORR	COUNTER	No	The number of successful reroutes due to ORR for this trunk group for the specified interval.
SUCCESSFUL_SORR	COUNTER	No	The number of successful reroutes due to SORR for this trunk group for the specified interval.
NO_UNRESERVED_CKT S	COUNTER	No	The current number of calls cancelled due to no unreserved circuits on an ingress trunk group for the specified interval.

Column Name	Column Type	Index	Description
IN_CALL_NO_CKTS	COUNTER	No	The current number of calls on an ingress trunk group that were cancelled due to no circuits for the specified interval.

IPMTRGIntervalStats

Column Name	Column Type	Index	Description
MTRM_PORT	INTEGER	Yes	Port number that uniquely identifies the MTRM (Master Trunk Group Manager) residing on the GSX.
MTRG_INDEX	INTEGER	Yes	Master Trunk Group Index unique on a GSX hosting MTRMs.
CONTRIBUTORS	INTEGER	No	Number of trunk groups that contributed to the row in IPMTRGIntervalStats DB table.
TG_IN_USAGE	COUNTER	No	The inbound usage for this trunk group for the specified interval. - For PSTN trunk groups, this equates to the time a trunk is seized to the time it is released. - For Selected IP Trunk Groups, this equates to the time media bandwidth is activated to the time it is deactivated. Note This field is applicable to SelectedIP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
TG_OUT_USAGE	COUNTER	No	The outbound usage for this trunk group for the specified interval. - For PSTN trunk groups, this equates to the time a trunk is seized to the time it is released. - For Selected IP trunk groups, this equates to the time media bandwidth is activated to the time it is deactivated. Note This field is applicable to SelectedIPTGs, but not LinkedIP TGs.
TG_IN_CALLS	COUNTER	No	The number of completed inbound calls on this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALLS	COUNTER	No	The number of completed outbound calls on this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALL_ATTEMPTS	COUNTER	No	The number of inbound call attempts on this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
TG_OUT_CALL_ATTEMPTS	COUNTER	No	The number of outbound call attempts on this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_MAX_COMPLETED_CALLS	COUNTER	No	The maximum number of completed calls in the inbound and outbound direction for this trunk group for the specified interval. Note This field is applicable to all TG types.
TG_TOTAL_CALL_SETUP_TIME	COUNTER	No	The total call setup time for all completed calls in the inbound and outbound directions for this trunk group for the specified interval measured in hundredths of a second. Use this object as the numerator for calculating average call setup time Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_CALL_SETUPS	COUNTER	No	The total number of calls setup but not necessarily completed in the inbound and outbound directions for this trunk group for the specified interval. Use this object as the denominator for calculating average call setup time. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
TG_IN_CALL_FAIL_NO_ROUTES	COUNTER	No	The number of inbound failed calls because there was no route available for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALL_FAIL_NO_RESOURCES	COUNTER	No	The number of inbound failed calls because there was an unavailable resource for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALL_FAIL_NO_SERVICE	COUNTER	No	The number of inbound failed calls because there was an unavailable service for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALL_FAIL_INVALID_CALL	COUNTER	No	The number of inbound failed calls because there was an invalid call attempt for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
TG_IN_CALL_FAIL_NW_FAILURE	COUNTER	No	The number of inbound failed calls because there was a network failure for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	The number of inbound failed calls because there was a protocol error for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALL_FAIL_UNSPECIFIED	COUNTER	No	The number of inbound failed calls for an unspecified reason for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALL_FAIL_NO_ROUTES	COUNTER	No	The number of outbound failed calls because there was no route available for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
TG_OUT_CALL_FAIL_NO_RESOURCES	COUNTER	No	The number of outbound failed calls because there was an unavailable resource for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALL_FAIL_NO_SERVICE	COUNTER	No	The number of outbound failed calls because there was an unavailable service for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALL_FAIL_INVALID_CALL	COUNTER	No	The number of outbound failed calls because there was an invalid call attempt for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	The number of outbound failed calls because there was a network failure for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
TG_OUT_CALL_FAIL_PROTOCOL_ERR	COUNTER	No	The number of outbound failed calls because there was a protocol error for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALL_FAIL_UNSPECIFIED	COUNTER	No	The number of outbound failed calls for an unspecified reason for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_AVG_CALL_SETUP_TIME	INTEGER	No	The average call setup time (in hundredths of a second) calculated as: $\text{TG\_TOTAL\_CALL\_SETUP\_TIME} / \text{TG\_CALL\_SETUPS}$
TG_INBOUND_BHA	INTEGER	No	This field is calculated as: $\text{TG\_IN\_CALL\_ATTEMPTS} * \text{NUM\_TG\_INTERVALS}$ where NUM_TG_INTERVALS = (60/ the size of the TG interval in minutes)
TG_OUTBOUND_BHA	INTEGER	No	This field is calculated as: $\text{TG\_OUT\_CALL\_ATTEMPTS} * \text{NUM\_TG\_INTERVALS}$ where NUM_TG_INTERVALS = (60/ the size of the TG interval in minutes)
MTRG_NAME	STRING	No	The name of the Master Trunk Group.

Column Name	Column Type	Index	Description
ROUTING_ATTEMPTS	COUNTER	No	The number of routing attempts for this trunk group for the specified interval. Note This field is applicable to all trunk group types.
ROUTING_FAILS_RESV	COUNTER	No	The number of routing failures due to no unreserved circuits for this trunk group for the specified interval. Note This field is applicable to all trunk group types.
SILC	COUNTER	No	The number of calls cancelled due to SILC for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
STRCANT	COUNTER	No	The number of calls cancelled due to STR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
STRSKIP	COUNTER	No	The number of calls skipped due to STR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
SKIP	COUNTER	No	The number calls skipped due to the SKIP traffic control for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
CANT	COUNTER	No	The number of calls cancelled due to CANT for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
CANF	COUNTER	No	The number of calls cancelled due to CANF for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
ROUTE_ATTEMPTS_IRR	COUNTER	No	The number of reroute attempts due to IRR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
ROUTE_ATTEMPTS_SIR R	COUNTER	No	The number of reroute attempts due to SIRR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
ROUTE_ATTEMPTS_ORR	COUNTER	No	The number of reroute attempts due to ORR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
ROUTE_ATTEMPTS_SORR	COUNTER	No	The number of reroute attempts due to SORR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
SUCCESSFUL_IRR	COUNTER	No	The number of successful reroutes due to IRR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
SUCCESSFUL_SIRR	COUNTER	No	The number of successful reroutes due to SIRR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
SUCCESSFUL_ORR	COUNTER	No	The number of successful reroutes due to ORR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
SUCCESSFUL_SORR	COUNTER	No	The number of successful reroutes due to SORR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TOTAL_USAGE_SECS	INTEGER	No	The total usage for this trunk group in seconds calculated as: (TG_IN_USAGE + TG_OUT_USAGE)
IN_BW_USAGE	COUNTER	No	The sum of BW usage (expected data rate in bits per second multiplied by call duration in seconds) for every inbound call associated with this trunk group for the specified interval. Note This field is only applicable to IP Trunk Groups.
OUT_BW_USAGE	COUNTER	No	The sum of BW usage (expected data rate in bits per second multiplied by call duration in seconds) for every outbound call associated with this trunk group for the specified interval. Note This field is only applicable to IP Trunk Groups.
MAX_ACTIVE_BW_USAGE	COUNTER	No	The high watermark of BW usage in either direction associated with this trunk group for the specified interval. Note This field is only applicable to IP Trunk Groups.

Column Name	Column Type	Index	Description
ALLOC_FAIL_BW_LIMIT	COUNTER	No	The number of BW Requests which fail because the configured bandwidth limit (SonusTgIpBandwidthLimit) has been exceeded for this trunk group for the specified interval. Note This field is only applicable to IP Trunk Groups.
ALLOC_FAIL_CALL_LIMIT	COUNTER	No	The number of BW Requests which fail because configured call limit (SonusTgIpCallLimit) has been exceeded for this trunk group for the specified interval. Note This field is only applicable to IP Trunk Groups.
ALLOC_FAIL_PARENT_TG_LIMIT	COUNTER	No	The number of BW Requests which fail because a configured call or bandwidth limit has been exceeded for one of this trunk group's parent trunk groups for the specified interval. This occurs only when an IP Trunk Group hierarchy has been established. Note This field is only applicable to IP Trunk Groups.
CALLS_WITH_PKT_OUTAGE	COUNTER	No	The number of calls with a maximum packet outage whose duration exceeds the configured minimum (SonusTgIpPacketOutageDetectionMinimumDuration) for this trunk group for the specified interval. Note This field is only applicable to SelectedIP TGs. It is not applicable to LinkedIP or Circuit TGs.

Column Name	Column Type	Index	Description
CALLS_WITH_PKT_OUTAGE_ATEND	COUNTER	No	The number of calls whose maximum packet outage occurs at the end of the call for this trunk group for the specified interval. This is likely an indication that the call terminated because of poor quality Note This field is only applicable to SelectedIP TGs. It is not applicable to LinkedIP or Circuit TGs.
TOTAL_PKT_OUTAGE	COUNTER	No	The summation of packet outage durations (in milliseconds) whose duration exceeds the configured minimum (SonusTgIpPacketOutageDetectionMinimumDuration), which is reported during the specified performance interval. Calculate the average packet outage duration by dividing this field by the number of calls reporting packet outages (SonusTrunkGroupCurrentCallsWithPktOutage). Note This field is only applicable to SelectedIP TGs. It is not applicable to LinkedIP or Circuit TGs.
MAX_PKT_OUTAGE	INTEGER	No	The single longest maximum reported packet outage duration (in milliseconds) experienced during the specified performance interval for this trunk group. Note This field is only applicable to SelectedIP TGs. It is not applicable to LinkedIP or Circuit TGs.

Column Name	Column Type	Index	Description
NUM_POD_EVENTS	COUNTER	No	The number of Packet Outage Detection (POD) Events detected for this trunk group for the specified interval. A POD event occurs when a configurable number of calls (<code>SonusTgIpPacketOutageDetectionMinimumCalls</code>) experience a packet outage with duration exceeding a programmable threshold (<code>SonusTgIpPacketOutageDetectionMinimumDuration</code>). Note This field is only applicable to SelectedIP TGs. It is not applicable to LinkedIP or Circuit TGs.
CALLS_PO_BUFFER_GOOD	COUNTER	No	Number of calls with all subintervals reporting GOOD playout buffer quality for this trunk group for the specified interval. Note This field is only applicable to SelectedIP TGs. It is not applicable to LinkedIP or Circuit TGs.
CALLS_PO_BUFFER_ACCEPTABLE	COUNTER	No	Number of calls with all subintervals reporting ACCEPTABLE or better playout buffer quality for this trunk group for the specified interval. Note This field is only applicable to SelectedIP TGs. It is not applicable to LinkedIP or Circuit TGs.

Column Name	Column Type	Index	Description
CALLS_PO_BUFFER_POOR	COUNTER	No	Number of calls with all subintervals reporting POOR or better playout buffer quality for this trunk group for the specified interval. Note This field is only applicable to SelectedIP TGs. It is not applicable to LinkedIP or Circuit TGs.
CALLS_PO_BUFFER_UNACCT	COUNTER	No	Number of calls with at least one subinterval reporting UNACCEPTABLE playout buffer quality for this trunk group for the specified interval. Note This field is only applicable to SelectedIP TGs. It is not applicable to LinkedIP.
NO_PSX_ROUTE	COUNTER	No	The current number of calls on an ingress trunk group that failed due to no routes returned from the PSX for the specified interval. Note This field is applicable to SelectedIP TGs, but not LinkedIP TGs.
CALLS_ABANDONED	COUNTER	No	The current number of calls on a trunk group that were abandoned while dialing for the specified interval. Note This field is applicable to SelectedIP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
DIRECTION	COUNTER	No	The direction of calls on this IP Tg. Possible values are: • 1 for inComing • 2 for outGoing • 3 bothWays
CIRCUITS	COUNTER	No	This field is calculated using the formula: if PSTN_TOTAL_AVAILABLE is not unlimited (unlimited is 1 setting) then circuits = (PSTN_TOTAL_AVAILABLE + PSTN_INBOUND_USAGE + PSTN_OUTBOUND_USAGE + PRIORITY_CALL_USAGE) where, PSTN_TOTAL_AVAILABLE = IP_CALL_LIMIT - TOTALUSAGE else circuits = unlimited (high value) and returns 1.

IPTrunkGroupIntervalStats

Note

Statistics in the IPTrunkGroupIntervalStats table apply only to IP Trunk Groups. Statistics for PSTN Trunk Groups are stored in the TrunkGroupIntervalStats table.

Note

It takes approximately 12 to 13:40 hours to reflect in the **RAMP** statistics export when the trunk group type is changed on the device for the same Trunk Group ID.

Column Name	Column Type	Index	Description
TG_INDEX	INTEGER	Yes	The index into the SonusTgTable
IP_TG_TYPE_CODE	INTEGER	No	The type of IP Trunk Group. Possible values: • 2 IP Selected • 3 IP Linked

Column Name	Column Type	Index	Description
TG_IN_USAGE	COUNTER	No	The usage in the inbound direction for this trunk group for the specified interval. For Selected IP Trunk Groups usage is defined as the time media bandwidth is activated to the time it is deactivated. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_USAGE	COUNTER	No	The usage in the outbound direction for this trunk group for the specified interval. For Selected IP Trunk Groups usage is defined as the time media bandwidth is activated to the time it is deactivated. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALLS	COUNTER	No	The number of completed inbound calls on this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALLS	COUNTER	No	The number of completed outbound calls on this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
TG_IN_CALL_ATTEMPTS	COUNTER	No	The number of inbound call attempts on this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALL_ATTEMPTS	COUNTER	No	The number of outbound call attempts on this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_MAX_COMPLETED_CALLS	INTEGER	No	The maximum number of completed calls in the inbound and outbound direction for this trunk group for the specified interval.
TG_TOTAL_CALL_SETUP_TIME	COUNTER	No	The total call setup time for all completed calls in the inbound and outbound directions for this trunk group for the specified interval measured in hundredths of a second. Use this object as the numerator for calculating average call set-up time. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_CALL_SETUPS	COUNTER	No	The total number of calls setup but not necessarily completed in the inbound and outbound directions for this trunk group for the specified interval. Use this object as the numerator for calculating average call set-up time. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
TG_IN_CALL_FAIL_NO_ROUTES	COUNTER	No	The number of inbound failed calls because there was no route available for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALL_FAIL_NO_RESOURCES	COUNTER	No	The number of inbound failed calls because there was an unavailable resource for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALL_FAIL_NO_SERVICE	COUNTER	No	The number of inbound failed calls because there was an unavailable service for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALL_FAIL_INV_ALID_CALL	COUNTER	No	The number of inbound failed calls because there was an invalid call attempt for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
TG_IN_CALL_FAIL_NW_FAILURE	COUNTER	No	The number of inbound failed calls because there was a network failure for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	The number of inbound failed calls because there was a protocol error for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_IN_CALL_FAIL_UNSPECIFIED	COUNTER	No	The number of inbound failed calls for an unspecified reason for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALL_FAIL_NO_ROUTES	COUNTER	No	The number of outbound failed calls because there was no route available for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
TG_OUT_CALL_FAIL_NO_RESOURCES	COUNTER	No	The number of outbound failed calls because there was an unavailable resource for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALL_FAIL_NO_SERVICE	COUNTER	No	The number of outbound failed calls because there was an unavailable service for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALL_FAIL_INVALID_CALL	COUNTER	No	The number of outbound failed calls because there was an invalid call attempt for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	The number of outbound failed calls because there was a network failure for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
TG_OUT_CALL_FAIL_PROTOCOL_ERR	COUNTER	No	The number of outbound failed calls because there was a protocol error for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_OUT_CALL_FAIL_UNSPECIFIED	COUNTER	No	The number of outbound failed calls for an unspecified reason for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
ROUTING_ATTEMPTS	COUNTER	No	The number of routing attempts for this trunk group for the specified interval.
ROUTING_FAILS_RESV	COUNTER	No	The number of routing failures due to no unreserved circuits for this trunk group for the specified interval.
SILC	COUNTER	No	The number of calls cancelled due to SILC for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
STRCANT	COUNTER	No	The number of calls cancelled due to STR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
STRSKIP	COUNTER	No	The number of calls skipped due to STR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
SKIP	COUNTER	No	The number calls skipped due to the SKIP traffic control for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
CANT	COUNTER	No	The number of calls cancelled due to CANT for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
CANF	COUNTER	No	The number of calls cancelled due to CANF for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
ROUTE_ATTEMPTS_IRR	COUNTER	No	The number of reroute attempts due to IRR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
ROUTE_ATTEMPTS_SIRR	COUNTER	No	The number of reroute attempts due to SIRR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
ROUTE_ATTEMPTS_ORR	COUNTER	No	The number of reroute attempts due to ORR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
ROUTE_ATTEMPTS_SORR	COUNTER	No	The number of reroute attempts due to SORR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
SUCCESSFUL_IRR	COUNTER	No	The number of successful reroutes due to IRR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
SUCCESSFUL_SIRR	COUNTER	No	The number of successful reroutes due to SIRR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
SUCCESSFUL_ORR	COUNTER	No	The number of successful reroutes due to ORR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
SUCCESSFUL_SORR	COUNTER	No	The number of successful reroutes due to SORR for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TG_AVG_CALL_SETUP_TIME	INTEGER	No	The average call setup time (in hundredths of a second) calculated as: $\text{TG\_TOTAL\_CALL\_SETUP\_TIME} / \text{TG\_CALL\_SETUPS}$
TG_INBOUND_BHA	INTEGER	No	This field is calculated as: $\text{TG\_IN\_CALL\_ATTEMPTS} * \text{NUM\_TG\_INTERVALS}$ where NUM_TG_INTERVALS = (60/ the size of the TG interval in minutes)
TG_OUTBOUND_BHA	INTEGER	No	This field is calculated as: $\text{TG\_OUT\_CALL\_ATTEMPTS} * \text{NUM\_TG\_INTERVALS}$ where NUM_TG_INTERVALS = (60/ the size of the TG interval in minutes)
TG_NAME	STRING	No	The trunk group name.
ACH_COUNT	INTEGER	No	Attempts (total) per Circuit per Hour a calculated field.
OCC_PERCENT	INTEGER	No	Occupancy (usage) percent a calculated field.

Column Name	Column Type	Index	Description
IN_CCH_COUNT	INTEGER	No	Incoming Connections (seizures) per Circuit per Hour a calculated field.
OUT_CCH_COUNT	INTEGER	No	Outgoing Connections (seizures) per Circuit per Hour a calculated field.
OFL_PERCENT	INTEGER	No	Overflow percentage a calculated field.
AVG_HT_MIN	FLOAT	No	Average Holding Time a calculated field.
AVG_DEL_SEC	FLOAT	No	Average Call Setup Delay (in seconds) a calculated field.
OUT_ASR_PERCENT	FLOAT	No	Outgoing Answer/Seizure Ratio percentage. Refer to Traffic Manager User Guide for the formula.
TOTAL_USAGE_SECS	INTEGER	No	The total usage for this trunk group in seconds calculated as: (TG_IN_USAGE + TG_OUT_USAGE)
IN_BW_USAGE	COUNTER	No	The sum of BW usage (expected data rate in bits per second multiplied by call duration in seconds) for every inbound call associated with this trunk group for the specified interval.
OUT_BW_USAGE	COUNTER	No	The sum of BW usage (expected data rate in bits per second multiplied by call duration in seconds) for every outbound call associated with this trunk group for the specified interval.
MAX_ACTIVE_BW_USAGE	COUNTER	No	The high watermark of BW usage in either direction associated with this trunk group for the specified interval.
ALLOC_FAIL_BW_LIMIT	COUNTER	No	The number of BW Requests which fail because the configured bandwidth limit (SonusTgIpBandwidthLimit) has been exceeded for this trunk group for the specified interval.
ALLOC_FAIL_CALL_LIMIT	COUNTER	No	The number of BW Requests which fail because configured call limit (SonusTgIpCallLimit) has been exceeded for this trunk group for the specified interval.

Column Name	Column Type	Index	Description
ALLOC_FAIL_PARENT_TG_LIMIT	COUNTER	No	The number of BW Requests which fail because a configured call or bandwidth limit has been exceeded for one of this trunk group's parent trunk groups for the specified interval. This occurs only when an IP Trunk Group hierarchy has been established.
CALLS_WITH_PKT_OUTAGE	COUNTER	No	The number of calls with a maximum packet outage whose duration exceeds the configured minimum (SonusTgIpPacketOutageDetectionMinimumDuration) for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
CALLS_WITH_PKT_OUTAGE_ATEND	COUNTER	No	The number of calls whose maximum packet outage occurs at the end of the call for this trunk group for the specified interval. This is likely an indication that the call terminated because of poor quality. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
TOTAL_PKT_OUTAGE	COUNTER	No	The summation of packet outage durations (in milliseconds) whose duration exceeds the configured minimum (SonusTgIpPacketOutageDetectionMinimumDuration), which is reported during the specified performance interval. Calculate the average packet outage duration by dividing this field by the number of calls reporting packet outages (SonusTrunkGroupCurrentCallsWithPktOutage). Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
MAX_PKT_OUTAGE	INTEGER	No	The single longest maximum reported packet outage duration (in milliseconds) experienced during the specified performance interval for this trunk group. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
NUM_POD_EVENTS	COUNTER	No	The number of Packet Outage Detection (POD) Events detected for this trunk group for the specified interval. A POD event occurs when a configurable number of calls (SonusTgIpPacketOutageDetectionMinimumCalls) experience a packet outage with duration exceeding a programmable threshold (SonusTgIpPacketOutageDetectionMinimumDuration). Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
CALLS_PO_BUFFER_GOOD	COUNTER	No	Number of calls with all subintervals reporting GOOD playout buffer quality for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
CALLS_PO_BUFFER_ACCEPTABLE	COUNTER	No	Number of calls with all subintervals reporting ACCEPTABLE or better playout buffer quality for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
CALLS_PO_BUFFER_POOR	COUNTER	No	Number of calls with all subintervals reporting POOR or better playout buffer quality for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
CALLS_PO_BUFFER_UNACCT	COUNTER	No	Number of calls with at least one subinterval reporting UNACCEPTABLE playout buffer quality for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
NO_PSX_ROUTE	COUNTER	No	The current number of calls on an ingress trunk group that failed due to no routes returned from the PSX for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
CALLS_ABANDONED	COUNTER	No	The current number of calls on a trunk group that were abandoned while dialing for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
DIRECTION	INTEGER	No	The value in this field is determined in the following manner: <pre> if(TWO_WAY_TOTAL_CONFIG > 0) {direction = 3; (i.e TWO WAY) } else if(ONE_WAY_IN_TOTAL_CONFIG > 0 && ONE_WAY_OUT_TOTAL_CONFIG > 0) {direction = 3; (i.e TWO WAY) } else if(ONE_WAY_IN_TOTAL_CONFIG > 0) {direction = 1; (i.e ONE WAY IN) } else if(ONE_WAY_OUT_TOTAL_CONFIG > 0) {direction = 2; (i.e ONE WAY OUT) } else {direction = 4; (i.e NOT CONFIGURED) </pre>
CIRCUITS	INTEGER	No	This field is calculated using the formula: $\text{ONE\_WAY\_IN\_TOTAL\_CONFIG} + \text{ONE\_WAY\_OUT\_TOTAL\_CONFIG} + \text{TWO\_WAY\_TOTAL\_CONFIG}$
CALL_COMPLETION_PERCENT	INTEGER	No	Percent of total (inbound and outbound) calls that completed. Calculated as: $((\text{TG\_IN\_CALLS} + \text{TG\_OUT\_CALLS}) * 100) / (\text{TG\_IN\_CALL\_ATTEMPTS} + \text{TG\_OUT\_CALL\_ATTEMPTS})$
IN_CALL_FAILS_PERCENT	INTEGER	No	Percent of Inbound calls failed. Calculated as follows: $(((\text{TG\_IN\_CALL\_FAIL\_NO\_ROUTES} + \text{TG\_IN\_CALL\_FAIL\_NO\_RESOURCES} + \text{TG\_IN\_CALL\_FAIL\_NO\_SERVICE} + \text{TG\_IN\_CALL\_FAIL\_INVALID\_CALL} + \text{TG\_IN\_CALL\_FAIL\_NW\_FAILURE} + \text{TG\_IN\_CALL\_FAIL\_PROTOCOL\_ERROR} + \text{TG\_IN\_CALL\_FAIL\_UNSPECIFIED} + \text{NO\_PSX\_ROUTE} + \text{NO\_UNRESERVED\_CKTS} + \text{IN\_CALL\_NO\_CKTS}) * 100) / \text{TG\_IN\_CALL\_ATTEMPTS})$

Column Name	Column Type	Index	Description
OUT_CALL_FAILS_PERCENT	INTEGER	No	Percent of Outbound calls failed. Calculated as follows: $\frac{((TG\_OUT\_CALL\_FAIL\_NO\_ROUTES + TG\_OUT\_CALL\_FAIL\_NO\_RESOURCES + TG\_OUT\_CALL\_FAIL\_NO\_SERVICE + TG\_OUT\_CALL\_FAIL\_INVALID\_CALL + TG\_OUT\_CALL\_FAIL\_NW\_FAILURE + TG\_OUT\_CALL\_FAIL\_PROTOCOL\_ERROR + TG\_OUT\_CALL\_FAIL\_UNSPECIFIED) * 100)}{TG\_OUT\_CALL\_ATTEMPTS}$
TOTAL_CALL_FAILS_PERCENT	INTEGER	No	Percent of total (inbound and outbound) calls failed. The summation of columns in IN_CALL_FAILS_PERCENT and OUT_CALL_FAILS_PERCENT
ROUTING_FAILS_PERCENT	INTEGER	No	Percent of routing attempts that failed. Calculated as: $\frac{(((ROUTING\_FAILS\_NO\_CKTS + ROUTING\_FAILS\_SFG + ROUTING\_FAILS\_RESV) * 100)}{ROUTING\_ATTEMPTS}$
CALLS_ABANDONED_PERCENT	INTEGER	No	Percent of calls that were abandoned while dialing. Calculated as follows: $\frac{((CALLS\_ABANDONED * 100)}{TG\_IN\_CALL\_ATTEMPTS}$
PLAYOUT_BUF_UNACCEPT_PERCENT	INTEGER	No	Percent of calls with at least one subinterval having unacceptable playout buffer quality. Calculated as follows: $\frac{((CALLS\_PO\_BUFFER\_UNACCT * 100)}{(TG\_IN\_CALLS + TG\_OUT\_CALLS)}$
AVG_PACKET_OUTAGE	INTEGER	No	Average packet outage duration in milliseconds. This is calculated as follows: $\frac{CALLS\_WITH\_PKT\_OUTAGE}{TOTAL\_PKT\_OUTAGE}$
TOTAL_PACKET_OUTAGE_PERCENT	FLOAT	No	Percent outage for all the calls. This value is usually much less than 1. Calculated as: $\frac{((TOTAL\_PKT\_OUTAGE * 100)}{((TG\_IN\_USAGE + TG\_OUT\_USAGE) * 1000)}$

Column Name	Column Type	Index	Description
FAIL_BW_LIMIT_PERCENT	INTEGER	No	Percent of bandwidth requests that fail because of configured bandwidth limit exceeded. Calculated as: $((\text{ALLOC\_FAIL\_BW\_LIMIT} * 100) / \text{ROUTING\_ATTEMPTS})$
FAIL_CALL_LIMIT_PERCENT	INTEGER	No	Percent of bandwidth requests that fail because of configured call limit exceeded. Calculated as: $((\text{ALLOC\_FAIL\_CALL\_LIMIT} * 100) / \text{ROUTING\_ATTEMPTS})$
FAIL_CALL_PARENT_TG_PERCENT	INTEGER	No	Percent of bandwidth requests that fail because of configured bandwidth or call limit exceeded on this trunk group's parent trunk groups. Calculated as: $((\text{ALLOC\_FAIL\_PARENT\_TG\_LIMIT} * 100) / \text{ROUTING\_ATTEMPTS})$
CALL_FAIL_POLICING	COUNTER	No	The number of calls on a trunk group that failed due to policing for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
SIPREG_ATTEMPTS	COUNTER	No	The number of SIP registration attempts on a trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
SIPREG_COMPLETIONS	COUNTER	No	The number of SIP registrations that have successfully completed on a trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
SIPREG_FAIL_POLICIN G	COUNTER	No	The number SIP registration attempts that failed due to policing on a trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
SIPREG_FAIL_INTERN AL	COUNTER	No	The number SIP registration attempts that failed due to internal reasons on a trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
SIPREG_FAIL_OTHER	COUNTER	No	The number SIP registration attempts that failed due to other reasons (signaling failures, etc.) on a trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
ACCCANT	COUNTER	No	The number of calls cancelled due to ACC for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.
ACCSKIP	COUNTER	No	The number of calls skipped due to ACC for this trunk group for the specified interval. Note This field is applicable to selected IP TGs, but not LinkedIP TGs.

Column Name	Column Type	Index	Description
INTERVAL_IN_ACTIVE_CALLS	INTEGER	No	The number of active incoming calls at the time of rollover from current statistics to interval statistics.
INTERVAL_OUT_ACTIVE_CALLS	INTEGER	No	The number of active outgoing calls at the time of rollover from current statistics to interval statistics.
INTERVAL_IN_ACTIVE_BW_USAGE	INTEGER	No	The amount of active incoming bandwidth usage at the time of rollover from current statistics to interval statistics.
INTERVAL_OUT_ACTIVE_BW_USAGE	INTEGER	No	The amount of active outgoing bandwidth usage at the time of rollover from current statistics to interval statistics.
INTERVAL_MAX_ROUTING_ATTEMPTS	INTEGER	No	The peak value of routing attempts in an interval. This field is applicable to both IPLINKED and IPSELECTED.
MAX_INGRESS_CALL_RATE	INTEGER	No	The peak number of inbound calls/sec that were successfully handled for the specified interval. This field is applicable to all trunk group types.
MAX_EGRESS_CALL_RATE	INTEGER	No	The peak number of outbound calls/sec that were successfully handled for the specified interval. This field is applicable to all trunk group types.
MAX_INGRESS_CALL_BURST_SIZE	INTEGER	No	The peak number of inbound calls/sec that were requested on a trunk group, including those that could not be successfully handled for the specified interval. This field is applicable to all trunk group types.
MAX_EGRESS_CALL_BURST_SIZE	INTEGER	No	The peak number of inbound calls/sec that were successfully handled for the specified interval. This field is applicable to all trunk group types.
TG_IN_PEAK_USAGE	INTEGER	No	The peak number of circuit usage in the inbound directions for this interval.
TG_OUT_PEAK_USAGE	INTEGER	No	The peak number of circuit usage in the outbound directions for this interval.

Column Name	Column Type	Index	Description
TG_TIME_IN_PEAK_USAGE_EB	STRING	No	The time of the peak number of circuit usage in the inbound directions for this interval.
TG_TIME_OUT_PEAK_USAGE_EB	STRING	No	The time of the peak number of circuit usage in the outbound directions for this interval.
TG_TIME_PEAK_USAGE_EB	STRING	No	The time of the peak number of circuit usage in the inbound and outbound directions for this interval.
IN_ASR_PERCENT	INTEGER	No	Incoming Answer/Seizure ratio. It is calculated in five minutes and 24 hour intervals, (Total Incoming Answer/Total Incoming Seizure*100) in the sample period. - Calculation for five minutes interval: (Total Incoming Answer/Total Incoming Seizure*100) in five minutes sample period. - Calculation for 24 hours interval: (Total Incoming Answer/Total Incoming Seizure*100) in 24 hours sample period.

PNSEnetStats

Column Name	Column Type	Index ?	Description
NIF_IFINDEX	INTEGER	Yes	NIF's ifIndex that identifies the NIF.
NIF_NUM_CALLS	INTEGER	No	The number of calls on this NIF.
NIF_CUR_BANDWIDTH	INTEGER	No	The current speed (bandwidth) allocated on this NIF.
NIF_MAX_BANDWIDTH	INTEGER	No	The maximum speed allowed on this NIF.
NIF_BANDWIDTH_USAGE	INTEGER	No	The % of available bandwidth that is in use.
NIF_SHELF	STRING	Yes	The shelf on which this interface exists.
NIF_SLOT	STRING	Yes	The slot on which this interface exists.

Column Name	Column Type	Index ?	Description
NIF_PORT	STRING	Yes	The port on which this interface exists.

SoftswitchStats

Column Name	Column Type	Index	Description
SS_INDEX	INTEGER	Yes	Identifies the Softswitch entry.
SS_OPER_STATE	INTEGER	No	The operational state of the Softswitch.
SS_AVG_TRANS_TIME	INTEGER	No	Records the average time taken in milliseconds for a Softswitch transaction.
SS_SERVER_RECONNECTS	COUNTER	No	The number of successful reconnections between the gateway and the Softswitch.
SS_TRANS_COMPLETED	COUNTER64	No	The number of successful transactions between the gateway and the Softswitch.
SS_TRANS_RETRY_ATTEMPTS	COUNTER	No	The number of transaction retries between the gateway and the Softswitch.
SS_TRANS_FAILED_ATTEMPTS	COUNTER	No	The number of unsuccessful transactions between the gateway and the Softswitch.
SS_VERSION	INTEGER	No	The negotiated protocol version between the gateway and the Softswitch.
SS_REDIRECT_REQUESTS	COUNTER	No	The cumulative number of redirect requests received from the Softswitch.
SS_RELEASE_REQUESTS	COUNTER	No	The cumulative number of release-call requests received from the Softswitch.
SS_DATA_REQUESTS	COUNTER	No	The cumulative number of data requests received from the Softswitch.
SS_QUERIES_SKIPPED_N_SERVICED	COUNTER	No	The cumulative number of Policy Requests serviced by the standby PSX while the active PSX experienced congestion.

Column Name	Column Type	Index	Description
SS_QUERIES_SKIPPED_N_REJECTED	COUNTER	No	The cumulative number of rejected Policy Requests while the active PSX is congested and a standby PSX is either congested or not available.
SS_CONGESTION_LEVEL	INTEGER	No	The PSX congestion level.
SS_ALLOWANCE_PERCENT	INTEGER	No	The PSX allowance percentage for the number of policy requests that the GSX skips. For example, an allowance of 75%, means that the GSX skips 1 out of every 4 policy requests. This allowance is provisioned on the PSX and enforced on the GSX when the PSX Congestion Control is enabled.
SS_NAME	STRING	No	The SoftSwitch name.

SystemStats

Column Name	Column Type	Index	Description
NODE_SHELF_INDEX	INTEGER	Yes	Identifies the target shelf. Returns the same value as SonusNodeShelfStatIndex, which was used to index into this table.
NODE_SLOT_INDEX	INTEGER	Yes	Identifies the target slot within the shelf.
NODE_TEMPERATURE	INTEGER	No	Indicates the current Celsius temperature being sensed by the server module in the indexed slot.
NODE_MEM_UTIL	INTEGER	No	The current memory utilization of this server module. The value returned is a number from 0 to 100, representing the percentage of memory utilization. Note that this number may be misleading considering many data structures are pre-allocated to ensure that the server modules maximum load capacity is achieved and maintained. This can result in relatively high memory utilizations under a low load.
NODE_CPU_UTIL	INTEGER	No	The current (at the time of the reading; not cumulative) CPU utilization of this server module. The value returned is a number from 0 to 100, representing the percentage of CPU utilization.

Column Name	Column Type	Index	Description
AVG_CPU_ONE_MIN	INTEGER	No	Indicates the average CPU utilization for the last minute.
AVG_CPU_FIVE_MINS	INTEGER	No	Indicates the average CPU utilization for the last five minutes.
AVG_MEM_ONE_MIN	INTEGER	No	Indicates the average memory utilization for the last minute.
AVG_MEM_FIVE_MINS	INTEGER	No	Indicates the average memory utilization for the last five minutes.

Note

File based collection (SFTP) includes slots that are enabled and ACTIVE.
 SNMP collection includes slots that are enabled irrespective of the status (ACTIVE or STANDBY).

TrunkGroupIntervalStats

Note

Statistics in the TrunkGroupIntervalStats table apply only to PSTN Trunk Groups. Statistics for IP Trunk Groups are stored in the IPTrunkGroupIntervalStats table.

Note

It takes approximately 12 to 13:40 hours to reflect in the **RAMP** statistics export when the trunk group type is changed on the device for the same Trunk Group ID.

Column Name	Column Type	Index	Description	canAggregate
TG_INDEX	INTEGER	Yes	The index into the SonusTgTable.	False
TG_IN_USAGE	COUNTER	No	The usage in the inbound direction for this trunk group for the specified interval. For PSTN trunk groups usage is defined as the time a trunk is seized to the time it is released.	False

Column Name	Column Type	Index	Description	canAggregate
TG_OUT_USAGE	COUNTER	No	The usage in the outbound direction for this trunk group for the specified interval. For PSTN trunk groups usage is defined as the time a trunk is seized to the time it is released.	False
TG_IN_CALLS	COUNTER	No	The number of completed inbound calls on this trunk group for the specified interval.	False
TG_IN_PEAK_USAGE	INTEGER	No	The peak number of circuit usage in the inbound directions for this interval.	True
TG_IN_PEAK_USAGE_EB	INTEGER	No	The time of the peak number of circuit usage in the inbound directions for this interval.	True
TG_OUT_CALLS	COUNTER	No	The number of completed outbound calls on this trunk group for the specified interval.	False
TG_OUT_PEAK_USAGE	INTEGER	No	The peak number of circuit usage in the outbound directions for this interval.	True
TG_OUT_PEAK_USAGE_EB	INTEGER	No	The time of the peak number of circuit usage in the outbound directions for this interval.	True
TG_IN_CALL_ATTEMPTS	COUNTER	No	The number of inbound call attempts on this trunk group for the specified interval.	False
TG_OUT_CALL_ATTEMPTS	COUNTER	No	The number of outbound call attempts on this trunk group for the specified interval.	False
TG_MAX_COMPLETED_CALLS	INTEGER	No	The maximum number of completed calls in the inbound and outbound direction for this trunk group for the specified interval.	False

Column Name	Column Type	Index	Description	canAggregate
TG_TOTAL_CALL_SETUP_TIME	COUNTER	No	The total call setup time for all completed calls in the inbound and outbound directions for this trunk group for the specified interval measured in hundredths of a second. Use this object as the numerator for calculating average call setup time	False
TG_CALL_SETUPS	COUNTER	No	The total number of calls setup but not necessarily completed in the inbound and outbound directions for this trunk group for the specified interval. Use this object as the numerator for calculating average call setup time.	False
TG_IN_CALL_FAIL_NO_ROUTES	COUNTER	No	The number of inbound failed calls because there was no route available for this trunk group for the specified interval.	False
TG_IN_CALL_FAIL_NO_RESOURCES	COUNTER	No	The number of inbound failed calls because there was an unavailable resource for this trunk group for the specified interval.	False
TG_IN_CALL_FAIL_NO_SERVICE	COUNTER	No	The number of inbound failed calls because there was an unavailable service for this trunk group for the specified interval.	False
TG_IN_CALL_FAIL_INVALID_CALL	COUNTER	No	The number of inbound failed calls because there was an invalid call attempt for this trunk group for the specified interval.	False
TG_IN_CALL_FAIL_NW_FAILURE	COUNTER	No	The number of inbound failed calls because there was a network failure for this trunk group for the specified interval.	False
TG_IN_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	The number of inbound failed calls because there was a protocol error for this trunk group for the specified interval.	False

Column Name	Column Type	Index	Description	canAggregate
TG_IN_CALL_FAIL_UNSPECIFIED	COUNTER	No	The number of inbound failed calls for an unspecified reason for this trunk group for the specified interval.	False
TG_OUT_CALL_FAIL_NO_ROUTES	COUNTER	No	The number of outbound failed calls because there was no route available for this trunk group for the specified interval.	False
TG_OUT_CALL_FAIL_NO_RESOURCES	COUNTER	No	The number of outbound failed calls because there was an unavailable resource for this trunk group for the specified interval.	False
TG_OUT_CALL_FAIL_NO_SERVICE	COUNTER	No	The number of outbound failed calls because there was an unavailable service for this trunk group for the specified interval.	False
TG_OUT_CALL_FAIL_INVALID_CALL	COUNTER	No	The number of outbound failed calls because there was an invalid call attempt for this trunk group for the specified interval.	False
TG_OUT_CALL_FAIL_NW_FAILURE	COUNTER	No	The number of outbound failed calls because there was a network failure for this trunk group for the specified interval.	False
TG_OUT_CALL_FAIL_PROTOCOL_ERR	COUNTER	No	The number of outbound failed calls because there was a protocol error for this trunk group for the specified interval.	False
TG_OUT_CALL_FAIL_UNSPECIFIED	COUNTER	No	The number of outbound failed calls for an unspecified reason for this trunk group for the specified interval.	False
TG_AVG_CALL_SETUP_TIME	INTEGER	No	The average call setup time (in hundredths of a second) calculated as: $\frac{\text{TG\_TOTAL\_CALL\_SETUP\_TIME}}{\text{TG\_CALL\_SETUPS}}$	False

Column Name	Column Type	Index	Description	canAggregate
TG_INBOUND_BHA	INTEGER	No	This field is calculated as: $\text{TG\_IN\_CALL\_ATTEMPTS} * \text{NUM\_TG\_INTERVALS}$ where NUM_TG_INTERVALS = (60/ the size of the TG interval in minutes)	False
TG_OUTBOUND_BHA	INTEGER	No	This field is calculated as: $\text{TG\_OUT\_CALL\_ATTEMPTS} * \text{NUM\_TG\_INTERVALS}$ where NUM_TG_INTERVALS = (60/ the size of the TG interval in minutes)	False
TG_NAME	STRING	No	The trunk group name.	False
TOTAL_USAGE_SECONDS	INTEGER	No	The amount of usage seconds, in both directions, for actual call traffic on a trunk group (TG_IN_USAGE+TG_OUT_USAGE).	False
CALL_COMPLETION_PERCENT	INTEGER	No	Percent of total (inbound and outbound) calls that completed. Calculated as: $((\text{TG\_IN\_CALLS} + \text{TG\_OUT\_CALLS}) * 100) / (\text{TG\_IN\_CALL\_ATTEMPTS} + \text{TG\_OUT\_CALL\_ATTEMPTS})$	False
ROUTING_ATTEMPTS	COUNTER	No	The number of routing attempts for this trunk group for the specified interval.	False
ROUTING_FAILS_NOCKTS	COUNTER	No	The number of routing failures due to no circuits available for this trunk group for the specified interval.	False
ROUTING_FAILS_SFG	COUNTER	No	The number of routing failures due to a simulated facility group at its capacity for this trunk group for the specified interval.	False
ROUTING_FAILS_RESV	COUNTER	No	The number of routing failures due to no unreserved circuits for this trunk group for the specified interval.	False

Column Name	Column Type	Index	Description	canAggregate
OUT_TRUNK_START_TIMEOUT	COUNTER	No	The number of outgoing trunk start timeouts for this trunk group for the specified interval.	False
SILC	COUNTER	No	The number of calls cancelled due to SILC for this trunk group for the specified interval.	False
STRCANT	COUNTER	No	The number of calls cancelled due to STR for this trunk group for the specified interval.	False
STRSKIP	COUNTER	No	The number of calls skipped due to STR for this trunk group for the specified interval.	False
SKIP	COUNTER	No	The number calls skipped due to the SKIP traffic control for this trunk group for the specified interval.	False
CANT	COUNTER	No	The number of calls cancelled due to CANT for this trunk group for the specified interval.	False
CANF	COUNTER	No	The number of calls cancelled due to CANF for this trunk group for the specified interval.	False
ACCCANT	COUNTER	No	The number of calls cancelled due to ACC for this trunk group for the specified interval.	False
ACCSKIP	COUNTER	No	The number of calls skipped due to ACC for this trunk group for the specified interval.	False
ROUTE_ATTEMPTS_IRR	COUNTER	No	The number of reroute attempts due to IRR for this trunk group for the specified interval.	False
ROUTE_ATTEMPTS_SIRR	COUNTER	No	The number of reroute attempts due to SIRR for this trunk group for the specified interval.	False

Column Name	Column Type	Index	Description	canAggregate
ROUTE_ATTEMPTS_ORR	COUNTER	No	The number of reroute attempts due to ORR for this trunk group for the specified interval.	False
ROUTE_ATTEMPTS_SORR	COUNTER	No	The number of reroute attempts due to SORR for this trunk group for the specified interval.	False
SUCCESSFUL_IRR	COUNTER	No	The number of successful reroutes due to IRR for this trunk group for the specified interval.	False
SUCCESSFUL_SIR R	COUNTER	No	The number of successful reroutes due to SIRR for this trunk group for the specified interval.	False
SUCCESSFUL_ORR	COUNTER	No	The number of successful reroutes due to ORR for this trunk group for the specified interval.	False
SUCCESSFUL_SOR R	COUNTER	No	The number of successful reroutes due to SORR for this trunk group for the specified interval.	False
NO_UNRESERVED _CKTS	COUNTER	No	The current number of calls cancelled due to no unreserved circuits on an ingress trunk group for the specified interval.	False
IN_CALL_NO_CKTS	COUNTER	No	The current number of calls on an ingress trunk group that were cancelled due to no circuits for the specified interval.	False

Column Name	Column Type	Index	Description	canAggregate
ACH_COUNT	INTEGER	No	Attempts (total) per Circuit per Hour. Shows the OUT number of call attempts being made on Trunk Groups. For PSTN Trunk Groups, this is valid for all incoming and outgoing Trunk Groups. It is calculated as: $\left(\frac{(\text{ROUTING\_ATTEMPTS} * 60)}{(\text{TWO\_WAY\_EQ\_TRUNKS\_OUT} * \text{TG\_INTERVAL\_SIZE})} \right)$ For IP Trunk Groups, ACH is calculated as : $\left(\frac{(\text{ROUTING\_ATTEMPTS} * 60)}{(\text{TOTAL\_IP\_TRUNKS} * \text{TG\_INTERVAL\_SIZE})} \right)$	False
OCC_PERCENT	INTEGER	No	Occupancy usage percentage. The percentage of trunks in a Trunk Group that are in use for supporting calls. For PSTN Trunk Groups, this is valid for all incoming and outgoing Trunk Groups, and is calculated as follows: $\left(\frac{(\text{TG\_IN\_USAGE} + \text{TG\_OUT\_USAGE}) * 100}{(\text{ACTUAL\_TRUNKS\_IN\_TG}) * 60 * (\text{tgIntervalSize})} \right)$ For IP Trunk Groups, this is calculated as follows: $\left(\frac{(\text{TG\_IN\_USAGE} + \text{TG\_OUT\_USAGE}) * 100}{(\text{TOTAL\_IP\_TRUNKS}) * 60 * (\text{tgIntervalSize})} \right)$	False

Column Name	Column Type	Index	Description	canAggregate
IN_CCH_COUNT	INTEGER	No	Incoming Connections (seizures) per Circuit per Hour. (The number of incoming call attempts being made on a Trunk Group. For PSTN Trunk Groups, this is valid for all incoming and outgoing Trunk Groups, and is calculated as follows: $\left(\frac{(TG\_IN\_CALL\_ATTEMPTS * 60)}{(TWO\_WAY\_EQ\_TRUNKS\_IN * (tgIntervalSize))} \right)$ For IP Trunk Groups, this is calculated as follows: $\left(\frac{(TG\_IN\_CALL\_ATTEMPTS * 60)}{(TOTAL\_IP\_TRUNKS * (tgIntervalSize))} \right)$	False
OUT_CCH_COUNT	INTEGER	No	Outgoing Connections (seizures) per Circuit per Hour. (For PSTN Trunk Groups, this is valid only for 2-way and outgoing 1-way TGs (not valid for incoming 1-way TGs), and is calculated as follows: $\left(\frac{(TG\_IN\_CALL\_ATTEMPTS * 60)}{(TWO\_WAY\_EQ\_TRUNKS\_OUT * (tgIntervalSize))} \right)$ For IP Trunk Groups, this is calculated as follows: $\left(\frac{(TG\_IN\_CALL\_ATTEMPTS * 60)}{(TOTAL\_IP\_TRUNKS * (tgIntervalSize))} \right)$	False
OFL_PERCENT	INTEGER	No	Overflow percentage. This is the overflowing of the TrunkGroup to other TrunkGroups lower down in a route list. For PSTN Trunk Groups, this is valid only for outgoing 1-way and 2-way TGs (not for incoming 1-way TGs), and is calculated as follows: $\left(\frac{(ROUTING\_FAILS\_NO\_CKTS * 100)}{ROUTING\_ATTEMPTS} \right)$ For IP TrunkGroups, this is calculated as: $\left(\frac{((ALLOC\_FAIL\_CALL\_LIMIT + ALLOC\_FAIL\_BW\_LIMIT) * 100)}{ROUTING\_ATTEMPTS} \right)$	False

Column Name	Column Type	Index	Description	canAggregate
AVG_HT_MIN	FLOAT	No	Average Holding Time. This is the average time calls that existed in the Trunk Group during the measurement interval (in 99.9 format). For PSTN Trunk Groups, this is valid for Trunk Groups (2W, Inc 1W, or Out 1W trunks), and is calculated as follows: $\left(\frac{\text{TG\_IN\_USAGE} + \text{TG\_OUT\_USAGE}}{(\text{TG\_IN\_CALL\_ATTEMPTS} + \text{TG\_OUT\_CALL\_ATTEMPTS}) * 60} \right)$	False
AVG_DEL_SEC	FLOAT	No	Average call setup delay, in seconds. This is the average amount of time it took to set up calls on a Trunk Group during the measurement interval (in 99.9 format). This is valid for all Trunk Groups(2W, Inc 1W, and Out 1W). It is same as TG_AVG_CALL_SETUP_TIME but stored with as float value higher precision. It is calculated as: $\left(\frac{\text{TG\_TOTAL\_CALL\_SETUP\_TIME}}{\text{TG\_CALL\_SETUPS}} \right)$	False
OUT_ASR_PERCENT	FLOAT	No	Outgoing Answer/Seizure ratio. This is percentage of calls on a Trunk Group that is successfully completed to answered state (in 99.9 % format). This is calculated as $\left(\frac{\text{TG\_OUT\_CALLS} * 100}{\text{TG\_OUT\_CALL\_ATTEMPTS}} \right)$	False
CIRCUITS	INTEGER	No	This field is calculated using the formula: $\text{ONE\_WAY\_IN\_TOTAL\_CONFIG} + \text{ONE\_WAY\_OUT\_TOTAL\_CONFIG} + \text{TWO\_WAY\_TOTAL\_CONFIG}.$	False

Column Name	Column Type	Index	Description	canAggregate
BLOCKED_CIRCUITS	INTEGER	No	This field is calculated using the formula: $\text{BLOCKED\_CIRCUITS} = (\text{CIRCUITS} - (\text{ONE\_WAY\_IN\_TOTAL\_AVAIL} + \text{ONE\_WAY\_IN\_USAGE} + \text{ONE\_WAY\_OUT\_TOTAL\_AVAIL} + \text{ONE\_WAY\_OUT\_USAGE} + \text{TWO\_WAY\_TOTAL\_AVAIL} + \text{TWO\_WAY\_USAGE}))$	False
DIRECTION	INTEGER	No	The value in this field is determined in the following manner: <pre> if(TWO_WAY_TOTAL_CONFIG > 0) {direction = 3; (i.e TWO WAY)} } else if(ONE_WAY_IN_TOTAL_CONFIG > 0 && ONE_WAY_OUT_TOTAL_CONFIG > 0) {direction = 3; (i.e TWO WAY)} } else if(ONE_WAY_IN_TOTAL_CONFIG > 0) {direction = 1; (i.e ONE WAY IN)} } else if(ONE_WAY_OUT_TOTAL_CONFIG > 0) {direction = 2; (i.e ONE WAY OUT)} } else {direction = 4; (i.e NOT CONFIGURED)} </pre>	False
NO_PSX_ROUTE	COUNTER	No	The current number of calls on an ingress trunk group that failed due to no routes returned from the PSX for the specified interval. Note This field is only applicable to Circuit TGs.	False

Column Name	Column Type	Index	Description	canAggregate
COT_IN_ATTEMPTS	COUNTER	No	The current number of inbound continuity tests for the specified interval. Note This field is only applicable to Circuit TGs.	False
COT_OUT_ATTEMPTS	COUNTER	No	The current number of outbound continuity tests for the specified interval. Note This field is only applicable to Circuit TGs.	False
COT_SUCCESS	COUNTER	No	The current number of successful continuity tests for the specified interval. Note This field is only applicable to Circuit TGs.	False
COT_FAILS	COUNTER	No	The current number of failed continuity tests for the specified interval. Note This field is only applicable to Circuit TGs.	False

Column Name	Column Type	Index	Description	canAggregate
COT_ABORTS	COUNTER	No	The current number of aborted continuity tests for the specified interval. Note This field is only applicable to Circuit TGs.	False
IN_GLARE_BLOCKED	COUNTER	No	The number of ingress calls on a trunk group that were blocked due to glare for the specified interval. This is calculated as follows: $((IN\_GLARE\_BLOCKED * 100) / TG\_IN\_CALL\_ATTEMPTS)$ Note This field is only applicable to Circuit TGs.	False
OUT_GLARE_BLOCKED	COUNTER	No	The number of egress calls on a trunk group that were blocked due to glare for the specified interval. $((OUT\_GLARE\_BLOCKED * 100) / TG\_OUT\_CALL\_ATTEMPTS)$ Note This field is only applicable to Circuit TGs.	False
GLARE_ENCOUNTED	COUNTER	No	The number of calls on a trunk group that encountered glare. Note This field is only applicable to Circuit TGs.	False

Column Name	Column Type	Index	Description	canAggregate
IN_ASR_PERCENT	Integer	NA	Incoming Answer/Seizure ratio. It is calculated in five minutes and 24 hour intervals, (Total Incoming Answer/Total Incoming Seizure*100) in the sample period. - Calculation for five minutes interval: (Total Incoming Answer/Total Incoming Seizure*100) in five minutes sample period. - Calculation for 24 hours interval: (Total Incoming Answer/Total Incoming Seizure*100) in 24 hours sample period.	False
CALLS_ABANDONED	COUNTER	No	The current number of calls on a trunk group that were abandoned while dialing for the specified interval. This is calculated as follows: $((\text{OUT\_GLARE\_BLOCKED} * 100) / \text{TG\_OUT\_CALL\_ATTEMPTS})$ Note This field is applicable to Circuit TGs and SelectedIP TGs, but not LinkedIP TGs.	False
IN_CALL_FAILS_PERCENT	INTEGER	No	Percent of Inbound calls failed. Calculated as follows: $((\text{TG\_IN\_CALL\_FAIL\_NO\_ROUTES} + \text{TG\_IN\_CALL\_FAIL\_NO\_RESOURCES} + \text{TG\_IN\_CALL\_FAIL\_INVALID\_CALL} + \text{TG\_IN\_CALL\_FAIL\_NW\_FAILURE} + \text{TG\_IN\_CALL\_FAIL\_PROTOCOL\_ERROR} + \text{TG\_IN\_CALL\_FAIL\_UNSPECIFIED} + \text{NO\_PSX\_ROUTE} + \text{NO\_UNRESERVED\_CKTS} + \text{IN\_CALL\_NO\_CKTS}) * 100) / \text{TG\_IN\_CALL\_ATTEMPTS})$	False

Column Name	Column Type	Index	Description	canAggregate
OUT_CALL_FAILS_PERCENT	INTEGER	No	Percent of Outbound calls failed. Calculated as follows: $\frac{((TG\_OUT\_CALL\_FAIL\_NO\_ROUTES + TG\_OUT\_CALL\_FAIL\_NO\_RESOURCES + TG\_OUT\_CALL\_FAIL\_NO\_SERVICE + TG\_OUT\_CALL\_FAIL\_INVALID\_CALL + TG\_OUT\_CALL\_FAIL\_NW\_FAILURE + TG\_OUT\_CALL\_FAIL\_PROTOCOL\_ERROR + TG\_OUT\_CALL\_FAIL\_UNSPECIFIED) * 100)}{TG\_OUT\_CALL\_ATTEMPTS}$	False

Column Name	Column Type	Index	Description	canAggregate
TOTAL_CALL_FAILS_PERCENT	INTEGER	No	Percent of total (inbound and outbound) calls failed. The summation of columns in IN_CALL_FAILS_PERCENT and OUT_CALL_FAILS_PERCENT $\frac{((TG\_IN\_CALL\_FAIL\_NO\_ROUTES + TG\_IN\_CALL\_FAIL\_NO\_RESOURCES + TG\_IN\_CALL\_FAIL\_INVALID\_CALL + TG\_IN\_CALL\_FAIL\_NW\_FAILURE + TG\_IN\_CALL\_FAIL\_PROTOCOL\_ERROR + TG\_IN\_CALL\_FAIL\_UNSPECIFIED + NO\_PSX\_ROUTE + TG\_IN\_CALL\_ATTEMPTS + TG\_OUT\_CALL\_FAIL\_NO\_ROUTES + TG\_OUT\_CALL\_FAIL\_NO\_RESOURCES + TG\_OUT\_CALL\_FAIL\_NO\_SERVICE + TG\_OUT\_CALL\_FAIL\_INVALID\_CALL + TG\_OUT\_CALL\_FAIL\_NW\_FAILURE + TG\_OUT\_CALL\_FAIL\_PROTOCOL\_ERROR + TG\_OUT\_CALL\_FAIL\_UNSPECIFIED + TG\_OUT\_CALL\_ATTEMPTS + IN\_CALL\_NO\_CKTS) * 100)}{(TG\_IN\_CALL\_ATTEMPTS + TG\_OUT\_CALL\_ATTEMPTS)}}$	False
ROUTING_FAILS_PERCENT	INTEGER	No	Percent of routing attempts that failed. Calculated as: $\frac{((ROUTING\_FAILS\_NO\_CKTS + ROUTING\_FAILS\_SFG + ROUTING\_FAILS\_RESV) * 100)}{ROUTING\_ATTEMPTS}}$	False
CALLS_ABANDONED_PERCENT	INTEGER	No	Percent of calls that were abandoned while dialing. Calculated as follows: $\frac{(CALLS\_ABANDONED * 100)}{TG\_IN\_CALL\_ATTEMPTS}}$	False

Column Name	Column Type	Index	Description	canAggregate
IN_GLARE_BLOCKED_PERCENT	INTEGER	No	Percent of inbound calls that were blocked due to glare. Calculated as follows: $((\text{IN\_GLARE\_BLOCKED} * 100) / \text{TG\_IN\_CALL\_ATTEMPTS})$	False
OUT_GLARE_BLOCKED_PERCENT	INTEGER	No	Percent of outbound calls that were blocked due to glare. Calculated as follows: $((\text{OUT\_GLARE\_BLOCKED} * 100) / \text{TG\_OUT\_CALL\_ATTEMPTS})$	False
FAILED_COT_PERCENT	INTEGER	No	Percent of COT (Continuity Tests) that failed. Calculated as follows: $((\text{COT\_FAILS} * 100) / (\text{COT\_IN\_ATTEMPTS} + \text{COT\_OUT\_ATTEMPTS}))$	False
TG_USAGE_EB	INTEGER	No	Trunk Group usage according to the Erlang-B formula calculated using instantaneous PSTN_INBOUND_USAGE (sonusTgPstnInboundUsage) and PSTN_OUTBOUND_USAGE (sonusTgPstnInboundUsage) values. TG_USAGE_EB is added in TrunkGroupIntervalStats, where as PSTN_INBOUND_USAGE and PSTN_OUTBOUND_USAGE are a part of TrunkGroupStats. Helper class is updated to calculate TG_USAGE_EB by fetching necessary data from “supporting” TrunkGroupStats. No of channels: $\text{PSTN\_INBOUND\_USAGE} + \text{PSTN\_OUTBOUND\_USAGE} + \text{PRIORITY\_CALL\_USAGE}$ Probability of blocking is User configured $\text{TG\_USAGE\_EB} = \text{fun\_erlangB}(\text{No of channels, Probability of blocking})$	False

Column Name	Column Type	Index	Description	canAggregate
TG_PEAK_USAGE_EB	INTEGER	No	Peak Trunk Group usage according to Erlang-B formula. This value is calculated based on TG_MAX_COMPLETED_CALLS (sonusTrunkGroupCurrentMaxCompletedCalls or sonusTrunkGroupIntervalMaxCompletedCalls) value. No of channels: TG_MAX_COMPLETED_CALLS Probability of blocking is User Configured TG_PEAK_USAGE_EB: fun_erlangB (No of channels, Probability of blocking)	False
TG_AVG_USAGE	INTEGER	No	The parameter sonusTrunkGroupIntervalAverageCalls or sonusTrunkGroupCurrentAverageCalls to reflect average usage for trunk group in seconds.	False
TG_AVG_USAGE_EB	INTEGER	No	Peak Trunk Group usage according to Erlang-B formula. This value is calculated based on value of TG_AVG_USAGE. No of channels: TG_AVG_USAGE TG_AVG_USAGE_EB: fun_erlangB (No of channels, Probability of blocking)	False
TG_USAGE_PERCENT_EB	INTEGER	No	Trunk Group usage in percentage. Calculated as follows: $(TG\_USAGE\_EB * 100) / TG\_PEAK\_CAPACITY\_EB$	False
TG_AVG_USAGE_PERCENT	INTEGER	No	Average usage for Trunk Group in percentage. Calculated as follows: $(TG\_AVG\_USAGE * 100) / PSTN\_TOTAL\_CONFIGURED$	False

Column Name	Column Type	Index	Description	canAggregate
TG_AVG_USAGE_PERCENT_EB	INTEGER	No	Peak Trunk Group Capacity according to Erlang-B formula in percentage. Calculated as follows: $(TG\_AVG\_USAGE\_EB * 100) / TG\_PEAK\_CAPACITY\_EB$	False
TG_PEAK_USAGE_PERCENT	INTEGER	No	Peak usage for Trunk Group. Calculated as follows: $(TG\_MAX\_COMPLETED\_CALLS * 100) / PSTN\_TOTAL\_CONFIGURED$ The value of TG_MAX_COMPLETED_CALLS is collected from TrunkGroupStats	False
TG_PEAK_USAGE_PERCENT_EB	INTEGER	No	Peak usage for Trunk Group in percentage. Calculated as follows: $(TG\_PEAK\_USAGE\_EB * 100) / TG\_PEAK\_CAPACITY\_EB$	False
TG_OUT_PEAK_USAGE	INTEGER	No	The interval peak number of circuit usage in the outbound directions.	True
TG_OUT_PEAK_USAGE_EB	INTEGER	No	The interval peak number of circuit usage in the outbound directions.	False
TG_TIME_PEAK_USAGE_EB	INTEGER	No	Time interval peak number of circuit usage in both inbound and outbound directions.	False
TG_PEAK_CAPACITY_EB	INTEGER	No	Peak Trunk Group Capacity according to the Erlang-B formula. This value is calculated based on PSTN_TOTAL_AVAILABLE (sonusTgPstnTotalAvailable) value. No of channels: PSTN_TOTAL_CONFIGURED TG_PEAK_CAPACITY_EB: $fun\_erlangB(\text{No of channels}, \text{Probability of blocking})$	False
INTERVAL_IN_ACTIVE_CALLS	INTEGER	No	The number of active incoming calls at the time of rollover from current statistics to interval statistics.	False

Column Name	Column Type	Index	Description	canAggregate
INTERVAL_OUT_ACTIVE_CALLS	INTEGER	No	The number of active outgoing calls at the time of rollover from current statistics to interval statistics.	False
INTERVAL_IN_ACTIVE_BW_USAGE	INTEGER	No	The amount of active incoming bandwidth usage at the time of rollover from current statistics to interval statistics.	False
INTERVAL_OUT_ACTIVE_BW_USAGE	INTEGER	No	The amount of active outgoing bandwidth usage at the time of rollover from current statistics to interval statistics.	False
INTERVAL_MAX_ROUTING_ATTEMPTS	INTEGER	No	The peak value of routing attempts in an interval. Note This field is applicable to both IPLINKED and IPSELECTED.	False
MAX_INGRESS_CALL_RATE	INTEGER	No	The peak number of inbound calls/sec that were successfully handled for the specified interval. Note This field is applicable to all trunk group types.	False
MAX_EGRESS_CALL_RATE	INTEGER	No	The peak number of outbound calls/sec that were successfully handled for the specified interval. Note This field is applicable to all trunk group types.	False

Column Name	Column Type	Index	Description	canAggregate
MAX_INGRESS_CALL_BURST_SIZE	INTEGER	No	The peak number of inbound calls/sec that were requested on a trunk group, including those that could not be successfully handled for the specified interval. Note This field is applicable to all trunk group types.	False
MAX_EGRESS_CALL_BURST_SIZE	INTEGER	No	The peak number of inbound calls/sec that were successfully handled for the specified interval. Note This field is applicable to all trunk group types.	False

TrunkGroupStats

Column Name	Column Type	Index	Description	canAggregate
PSTN_STATUS_INDEX	INTEGER	Yes	A unique value for each trunk group between 1 and maximum allowed.	false
PSTN_TOTAL_AVAILABLE	INTEGER	No	The sum of all available or unblocked PSTN channels for this trunk group.	true
PSTN_INBOUND_RESERVED	INTEGER	No	It is applicable only for PSTN trunk groups that are configured for inbound or both directions only. This is the reserved count as specified by the percentage configured for this trunk group.	true
PSTN_INBOUND_USAGE	INTEGER	No	It is applicable only for PSTN trunk groups that are configured for inbound or both directions. This reflects the current inbound or incoming usage count of this trunk group.	true

Column Name	Column Type	Index	Description	canAggregate
PSTN_OUTBOUND_USAGE	INTEGER	No	It is applicable only for PSTN trunk groups that are configured for outbound or both directions. This reflects the current outbound, outgoing or non-priority usage count of this trunk group.	true
PSTN_TOTAL_CONFIGURED	INTEGER	No	The sum of all configured and registered PSTN channels for this trunk group.	true
PRIORITY_CALL_USAGE	INTEGER	No	It is applicable only for ISUP trunk groups that are configured and when SonusTgCirResvState is enabled. This reflects the current priority usage count of this trunk group.	true
PSTN_OUTBOUND_RSV	INTEGER	No	It is applicable only for PSTN trunk groups that are configured for ingoing call reservation. This is the reserved count as specified by the percentage configured for this trunk group.	true
ONE_WAY_IN_TOTAL_CONFIG	INTEGER	No	The sum of all configured and registered one way inbound PSTN channels for this trunk group.	true
ONE_WAY_IN_TOTAL_AVAIL	INTEGER	No	The sum of all available or unblocked one way inbound PSTN channels for this trunk group.	true
ONE_WAY_IN_USAGE	INTEGER	No	It is applicable only for PSTN trunk groups that are configured for one way inbound direction. This reflects the current one way inbound usage count of this trunk group.	true
ONE_WAY_OUT_TOTAL_CONFIG	INTEGER	No	The sum of all configured and registered one way outbound PSTN channels for this trunk group.	true
ONE_WAY_OUT_TOTAL_AVAIL	INTEGER	No	The sum of all available or unblocked one way outbound PSTN channels for this trunk group.	true

Column Name	Column Type	Index	Description	canAggregate
ONE_WAY_OUT_USAGE	INTEGER	No	It is applicable only for PSTN trunk groups that are configured for one way outbound direction. This reflects the current one way outbound usage count of this trunk group.	true
TWO_WAY_TOTAL_CONFIG	INTEGER	No	The sum of all configured and registered two way PSTN channels for this trunk group.	true
TWO_WAY_TOTAL_AVAIL	INTEGER	No	The sum of all available or unblocked two way PSTN channels for this trunk group.	true
TWO_WAY_USAGE	INTEGER	No	It is applicable only for PSTN trunk groups that are configured for two way. This reflects the current two way usage count of this trunk group.	true
BW_CURRENT_LIMIT	INTEGER	No	This is the current bandwidth limit for this trunk group. It is initial set to the configured bandwidth limit but may be reduced due to packet outage detection events.	true
BW_AVAILABLE	INTEGER	No	The amount of bandwidth available for allocation.	true
BW_INBOUND_USAGE	INTEGER	No	The amount of bandwidth in use for inbound traffic.	true
BW_OUTBOUND_USAGE	INTEGER	No	The amount of bandwidth in use for outbound traffic.	true

Insight Statistics

In this section:

- [InsightApplResUsageStats](#)
- [InsightFsUsageStats](#)
- [InsightHostUsageStats](#)

InsightApplResUsageStats

Column Name	Column Type	Index	Description
PID	GAUGE	Yes	The application process ID.
EXEC_NAME	STRING	No	The application executable name.
CPU_USAGE	INTEGER	No	The application CPU usage in percentage.
MEM_SIZE	GAUGE	No	The application physical memory size in kilobytes.
VMSIZE	GAUGE	No	The application virtual memory usage in kilobytes.

Note

Not applicable for RAMP CNF deployment.

InsightFsUsageStats

Column Name	Column Type	Index	Description
PATH_NAME	STRING	Yes	The File System Path Name.
USAGE	INTEGER	No	The File System Usage in percentage.

Note

The data reported in `InsightFSUsageStats` may differ with the output of Linux "df" command.

PM exported `InsightFsUsageStats` data may not be equal to Linux "df" command output. It calculates the usage percentage as $(\text{total\_space} - \text{available\_space}) / \text{total\_space} * 100$, which is not always equal to Linux df output.

Example:

```
[root@emshp7 tmp]# df -h /var
```

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/mapper/vg00-lv.var	50G	386M	47G	1%	/var

Even though only 386 MB out of 50 GB is used, the usage percentage is still 1% which is the percentage of reported for Used size with reference to Total size.

However, the Ribbon Application Management Platform (RAMP) calculates the usage percentage as $\text{total-available/total} * 100$. In this example, it is $50\text{GB}-47\text{GB}/50\text{GB} * 100 = 6\%$. RAMP calculates the effective usage.

In Linux, the missing space is interpreted as minfree percentage of reserved filesystem disk blocks. A typical filesystem value for minfree is 5% reserved to superuser processes.

Root can make use of all of the disk space but non-root processes will be restricted by the minfree value.

If a user or user process fills up a partition the root user can still create files within the provided space.

Keeping a minfree reserved is one way to ensure a sufficient amount of disk space for the filesystem to operate at high efficiency.

InsightHostUsageStats

Column Name	Column Type	Index	Description
CPU_AVG_USAGE	INTEGER	No	The average CPU usage percentage (rounded to the nearest integer) averaged over a 5 minute interval. The averaging is performed at the end of the interval. The CPU usage is calculated using this formula: $(\text{user time} + \text{kernel time}) / (\text{user time} + \text{kernel time} + \text{IO wait time} + \text{idle time}) * 100$. The sampling period is 5 seconds.
MEM_USAGE	INTEGER	No	The average host physical memory usage percentage (rounded to the nearest integer) averaged over a 5 minute interval. The averaging is performed at the end of the interval. The usage value is calculated by dividing total inuse memory by total physical memory in the system. The sampling period is 5 seconds.
SWAP_SPACE_USAGE	INTEGER	No	The average host swap space usage percentage (rounded to the nearest integer) averaged over a 5 minute interval. The averaging is performed at the end of the interval. The usage value is calculated by dividing total inuse swap space by total available swap space. The usage value is represented as a percentage and is rounded to the nearest integer!. The sampling period is 5 seconds.
PEAK_CPU_USAGE	INTEGER	No	The peak CPU usage percentage (round up to integer) during the interval.
PEAK_MEM_USAGE	INTEGER	No	The peak host physical memory usage percentage during the interval.

Column Name	Column Type	Index	Description
PEAK_SWAP_SPACE_USAGE	INTEGER	No	The peak swap space usage percentage during the interval.

Note

Not applicable for RAMP CNF deployment.

Note

`InsightHostUsageStats` collection supports only 5 minutes hard-coded polling interval and the statistics are collected every 5 minutes from RAMP. The `InsightHostUsageStats` collection interval cannot be changed.

PSX Statistics

In this section:

- [ApplResUsage](#)
- [DSPResDsp](#)
 - [GsmMapStats](#)
- [HostFileUsage](#)
- [HostSystemUsage](#)
- [Lnp](#)
- [PolicyRequestStats](#)
- [PSXAda](#)
 - [PSXAdaLookupStats](#)
 - [PSXAdaDcStats](#)
- [PSXCpsLicenseCountersStats](#)
- [PSXEscapeServices](#)
 - [PSXEscapeServiceStats](#)
 - [PSXEscapeServiceStats_AG](#)
- [PSXHpc](#)
 - [PSXHpcCallStats](#)
 - [PsxHpcGetsZoneStats](#)
 - [PSXHPCGetsCounterStats](#)
 - [PsxHpcGetsServerStats](#)
 - [PSXHpcSipeReqRecvStats](#)
 - [PSXHpcSipeRespSentStats](#)
- [PSXHTTP](#)
 - [PsxHTTPCCounterStats](#)
 - [PsxHttpClientInternalStats](#)
 - [PSXHTTPClientRESTServiceCountersStats](#)

- PSXHTTPClientRESTServiceFailureCountersStats
- PSXHttpPerIpStats
- PSXHTTPPerSvrTypeFailureCountersStats
- PSXHTTPPerSvrTypeInternalCountersStats
- PSXHTTPPerSvrTypeSignVerCounterStats
- PSXHttpSigningFailStats
- PSXHttpSigningStats
- PSXHttpVerificationStats
- PSXInd
 - PSXINDCALLSVCTYPESIPSERVERSIPSTATS
 - PSXIndSIPServerSIPStats
 - PSXIndividualPSXSIPStats
- PSXLnpPerSipServerCountersStats
- PSXNumCallsRecordedCRCStats
- PSXOutgoingLicStats
- PSXPeerOverloadThrottlingStats
- PsxPerFqdnCounterStats
- PSXPes
 - PSXPesCallServiceTypeStats
 - PSXPesCapCountersStats
 - PSXPesDscNpCountersStats
 - PSXPesEnumSrcNumberCountersStats
 - PSXPesFailureStats
 - PSXPesLcrStats
 - PSXPesPerServiceCountersStats
 - PSXPesStiRcdCountersStats
 - PSXPesStiShakenRcdCountersStats
 - PSXPesStiShakenCountersStats
 - PSXPesTranslationLookupCounters
- PSXScpa
 - PSXScpaSipPerServerStats
 - PSXScpaSipReqRespStats
 - PSXScpaSipStats
 - PSXScpaSuaAssocStats
 - PSXScpaSuaExtAssocStats
 - PSXScpaSuaProtocolStats
 - PSXScpaSuaRoutingStats
 - PSXScpaSuaSSNStats
- PSXSipeDnsStats
- PSXSipInternetworkingStats
- PSXSoftswitch
 - PSXSoftSwitchHTTPClientPeakCPSUsageCountersStats
 - PSXSoftSwitchHttpRestUsagePerServiceCountersStats
 - PSXSoftSwitchPesLicenseCountersStats

- PSXSoftSwitchScpaltuStats
- PSXSoftSwitchDIMASStats
- PSXSoftSwitchDrmReqCountersStats
- PSXSoftSwitchPesDnsEnumStats
- PSXSsPesInboundEnumStats
- PsxStirShakenStats
- PSXTM
 - PSXTMCdDNDestAllowStats
 - PSXTMCdDNDestBlockStats
 - PSXTMContractorOrigBlockStats
- PSXTMCPEGroup
 - PSXTMCPEGroupPreProcessingAllowedStats
 - PSXTMCPEGroupPreProcessingBlockedStats
 - PSXTMCPEGroupPreRoutingAllowedStats
 - PSXTMCPEGroupPreRoutingBlockedStats
 - PSXTMCPEGroupPostRoutingAllowedStats
 - PSXTMCPEGroupPostRoutingBlockedStats
- PSXTMHpcExemptionStats
- PSXTriggeredService
 - PSXTriggeredServiceStats
 - PSXTriggeredServiceStats_AG
 - PsxVerificationFailStats
- ScpaStats
- ServiceUsageStats
- SoftSwitchLwresd
 - SoftSwitchLwresdServerStats
 - SoftSwitchLwresdZoneStats
 - SoftSwitchPesMWIServiceStats
- SoftswitchScpa
 - SoftSwitchScpaAnsiTcStats
 - SoftSwitchScpaSpasStats
 - SoftSwitchScpaTtcTcStats
- SoftswitchSipe
 - SoftSwitchSipeMiscStats
 - SoftSwitchSipeProxyReqSentStats
 - SoftSwitchSipeProxyRspRcvdStats
 - SoftSwitchSipeReqRcvdStats
 - SoftSwitchSipeRspSentStats
 - SoftSwitchSipeSumStats
- TmCalling
 - TmCallingNumberAllowedStats
 - TmCallingNumberBlockedStats
- TmDialed
 - TmDialedDestAllowedStats
 - TmDialedDestBlockedStats
- TMFinal
 - TMFinalCallingNumAllowedStats

- TMFinalCallingNumBlockedStats
- TMFinalDestinationAllowedStats
- TMFinalDestinationBlockedStats
- TMTrans
 - TmTransDestAllowedStats
 - TmTransDestBlockedStats
- TollFreeStats

ApplResUsage

Column Name	Column Type	Index	Description
APPL_PID	GAUGE	Yes	Application process ID (PID)
EXE_NAME	STRING	No	Application executable name
CPU_USAGE_PERCENT	INTEGER	No	Application CPU usage in percent
MEM_USAGE	GAUGE	No	Application physical memory size in Kilobytes
VM_SIZE	GAUGE	No	Application virtual memory usage size in Kilobytes

DSPResDsp

GsmMapStats

Column Name	Column Type	Index	Description
SRI_REQUESTS	COUNTER	No	Number of Send Routing Information Request messages sent by the PSX.
SRI_ROUTE_RESPONSES	COUNTER	No	Number of Send Routing Information Response messages received by the PSX containing call delivery data.
SRI_FWD_RESPONSES	COUNTER	No	Number of Send Routing Information Response messages received by the PSX containing immediate call forwarding data.
SRI_ERRORS	COUNTER	No	Number of Send Routing Information fatal errors processed by the PSX.

Column Name	Column Type	Index	Description
SRI_TIMEOUT	COUNTER	No	Number of Send Routing Information Request messages that timed out without a response.
SRI_OR_REQUESTS	COUNTER	No	Number of Send Routing Information Request messages for Optimal Routing sent by the PSX.
RCH_REQUESTS	COUNTER	No	Number of Resume Call Handling Request messages received by the PSX.
RCH_ERRORS	COUNTER	No	Number of Resume Call Handling Request message fatal errors detected by the PSX.
SRI_TOTAL_RESPONSES	COUNTER	No	The total number of Send Routing Information responses received by the PSX.
MTRRSRI_REQUESTS	COUNTER	No	Number of Resume Call Handling Request with MTRR messages received by the PSX.
MTRRSRI_RESPONSES	COUNTER	No	Number of Resume Send Routing Information responses with MTRR received by the PSX.
MTRRRCH_REQUESTS	COUNTER	No	Number of Resume Call Handling Request messages with MTRR received by the PSX.
MAPATI_REQUESTS	COUNTER	No	Number of MAP ATI Request messages sent by the PSX.
MAPATIACK_RESPONSES	COUNTER	No	Number of MAP ATI ACK Response received by the PSX containing call delivery data.
MAPATI_ERRORS	COUNTER	No	Number of MAP ATI fatal errors processed by the PSX.
MAPATI_TIMEOUT	COUNTER	No	Number of MAP ATI Request messages that timed out without a response.

HostFileUsage

Column Name	Column Type	Index	Description
PATH_NAME	STRING	Yes	File System Path Name
USAGE_PERCENT	INTEGER	No	File system usage in percentage

HostSystemUsage

Column Name	Column Type	Index	Description
AVG_CPU_USAGE	INTEGER	No	The average CPU usage percentage (rounded to the nearest integer) averaged over a 5-minute interval. The averaging is performed at the end of the interval. The CPU usage is calculated using this formula: $(\text{user time} + \text{kernel time}) / (\text{user time} + \text{kernel time} + \text{IO wait time} + \text{idle time}) * 100$. The sampling period is 5 seconds.
MEM_USAGE_PERCENT	INTEGER	No	Average host physical memory usage percentage (rounded to the nearest integer) averaged over a 5-minute interval. The averaging is performed at the end of the interval. The usage value is calculated by dividing total inuse memory by total physical memory in the system. The sampling period is 5 seconds.
SWAP_USAGE_PERCENT	INTEGER	No	Average host swap space usage percentage (rounded to the nearest integer) averaged over a 5-minute interval. - The averaging is performed at the end of the interval. - The usage value is calculated by dividing total inuse swap space by total available swap space. - The usage value is represented as a percentage and is rounded to the nearest integer!. The sampling period is 5 seconds.
PEAK_CPU_USAGE	INTEGER	No	Peak CPU usage percentage (round up to integer) during the interval.

Column Name	Column Type	Index	Description
PEAK_MEM_USAGE	INTEGER	No	Peak host physical memory usage percentage during the interval.
PEAK_SWAP_SPACE_USAGE	INTEGER	No	Peak swap space usage percentage during the interval.

Note

HostSytemUsage Statistics collection supports only a 5-minutes hard-coded polling interval. Statistics are collected every 5 minutes from the PSX. The HostSytemUsage Statistics collection interval is not editable.

Lnp

Column Name	Column Type	Index	Description
GSX_IP	IPADDRESS	Yes	The GSX IP address to which the LNP Counters apply
GSX_NAME	STRING	No	The GSX Name to which the LNP Counters apply
NUM_MISROUTED_CALLS	COUNTER	No	Misrouted calls: Number of LNP-specific ISUP release messages received by the GSX9000 with cause 26 - misrouted call to a ported number.
NUM_INVALID_NUMBERS	COUNTER	No	Invalid Number: Number of LNP-specific ISUP release messages received by the GSX9000 with cause 28 - Invalid number format.

Column Name	Column Type	Index	Description
NUM_LNP_REQUESTS	COUNTER	No	Number of requests that need LNP: Total number of requests received by the Ribbon SoftSwitch which require LNP translation.

Column Name	Column Type	Index	Description
NUM_SCP_REQUESTS	COUNTER	No	Number of LNP requests sent to SCP: Total number of requests sent to the SCP for LNP translation.
NUM_DN_REQUESTS	COUNTER	No	Number of LNP requests to ported DNS: The number of LNP requests made for ported DNS.
NUM_REQUESTS_TIME DOUT	COUNTER	No	Number of timed out LNP requests: Number of LNP requests that timed out.
NUM_REQUEST_ERRO RS	COUNTER	No	Number of LNP request Errors: Number of errors other than timeout received from the SCP.

LnpGwStatsLnpStats

PolicyRequestStats

Column Name	Column Type	Index	Description
NUM_REQUESTS_NO_EX T_SVC	COUNTER	No	Total Requests (no ext service): Total number of policy requests (excluding those that needed external services, such as an SCP lookup) which were handled by the Soft Switch. Requests which timed out at the external interface are counted here.
TOTAL_TIME_NO_EXT_S VC	COUNTER	No	Total time (no ext service): Total time (number of milliseconds) taken to process these requests including requests that timed out at the external interface are also counted here.
AVG_TIME_NO_EXT_SVC	GAUGE	No	Average Time: Average amount of time (in milliseconds) taken to process each individual request. This is the average of the differences between the time a request was received and the time that the corresponding response was sent out.

Column Name	Column Type	Index	Description
NUM_REQUESTS_EXT_SVC	COUNTER	No	Total requests (External Svc): The number of requests which used an external service. Currently the features which use external services are LNP, Toll Free, CNAM, Conv TCAP, IS41, GSM MAP, SPAS, SIP SCP
TOTAL_TIME_EXT_SVC	COUNTER	No	Total time: Total time (in milliseconds) it took to process the requests that required an external service. This time includes the time it took for the external service to execute. This time does not include requests that timed out.
AVG_TIME_EXT_SVC	GAUGE	No	Average: Average time (in milliseconds) it took to process each of these requests.
TOTAL_TIME_EXT_PROC_SVC	COUNTER	No	Ex time: Total time (in milliseconds) it took in the external service to process all of these requests.
AVG_TIME_EXT_PROC_SVC	GAUGE	No	Ave Ex Time: Average time (in milliseconds) that it took in the external service to process each request.
NUM_TIMEOUTS	COUNTER	No	Total T/O: Total number of external service requests which timed out.
TOTAL_TIME_TIMEOUTS	COUNTER	No	Total time: Total time (in milliseconds) taken to process the timed out requests in the Softswitch. This total includes the timeout interval and the processing time.
AVG_TIME_TIMEOUTS	GAUGE	No	Average (Time in milliseconds): Average time taken to process each timed out request. This time includes the timeout interval and the processing time.
NUM_NON_POLICY_REQUESTS	COUNTER	No	Total non ss requests: Counts the total number of nonpolicy requests. These include heart beat (keep Alive) messages.

Column Name	Column Type	Index	Description
TOTAL_TIME_NON_POLICY_REQUESTS	COUNTER	No	Total time: Total time (in milliseconds) it took to process these nonpolicy requests.
AVG_TIME_NON_POLICY_REQUESTS	GAUGE	No	Average (Time in milliseconds): The average time in milliseconds it took to process each of these nonpolicy requests.

PSXAda

PSXAdaLookupStats

Column Name	Column Type	Index	Description
SUCCESSFUL_LOOKUPS	COUNTER	No	Number of successful AD Lookups.
FAILED_LOOKUPS	COUNTER	No	Number of Failed AD Lookups.

PSXAdaDcStats

Column Name	Column Type	Index	Description
NAME	STRING	Yes	The name of the Domain Controller .
CONNECTION_STATUS	GAUGE	No	Connection status of the Domain Controller, 0-UP and 1-DOWN
SYNC_STATUS	GAUGE	No	Sync status of the Domain Controller, 0-Synced and 1-Sync Failed.
LAST_SYNC_TIME	TIMETICKS	No	The Last Sync time from Domain Controller.

PSXCpsLicenseCountersStats

Column Name	Column Type	Index	Description	canAggregate	canAggregateType
CPS_LIC_DPLUS	INTEGER	No	The CPS license capacity for D+ Interface	False	SUM
ACC_CPS_LIC_DPLUS	COUNTER	No	The total number of calls accepted for D+ Interface with CPS-based licensing enforced	True	SUM
REJ_CPS_LIC_DPLUS	COUNTER	No	The total number of calls rejected for D+ Interface with CPS-based licensing enforced	True	SUM
CPS_LIC_SIPE	INTEGER	No	The CPS license capacity for Sipe Interface	False	SUM
ACC_CPS_LIC_SIPE	COUNTER	No	The total number of calls accepted for Sipe Interface with CPS-based licensing enforced	True	SUM
REJ_CPS_LIC_SIPE	COUNTER	No	The total number of calls rejected for Sipe Interface with CPS-based licensing enforced	True	SUM
CPS_LIC_ENUME	INTEGER	No	The CPS license capacity for Enum Interface	False	SUM
ACC_CPS_LIC_ENUME	COUNTER	No	The total number of calls accepted for Enum Interface with CPS-based licensing enforced	True	SUM
REJ_CPS_LIC_ENUME	COUNTER	No	The total number of calls rejected for Enum Interface with CPS-based licensing enforced.	True	SUM
INT_ACC_CPS_DPLUS	INTEGER	No	The total number of accepted D+ traffic per second with CPS-based licensing enforced	True	SUM
INT_REJ_CPS_DPLUS	INTEGER	No	The total number of rejected D+ traffic per second with CPS-based licensing enforced	True	SUM
INT_ACC_CPS_SIPE	INTEGER	No	The total number of accepted Sipe traffic per second with CPS-based licensing enforced	True	SUM
INT_REJ_CPS_SIPE	INTEGER	No	The total number of rejected Sipe traffic per second with CPS-based licensing enforced	True	SUM
INT_ACC_CPS_ENUME	INTEGER	No	The total number of accepted Enum traffic per second with CPS-based licensing enforced	True	SUM

Column Name	Column Type	Index	Description	canAggregate	canAggregateType
INT_REJ_CPS_ENUME	INTEGER	No	The total number of rejected Enum traffic per second with CPS-based licensing enforced	True	SUM
BASE_SW	INTEGER	No	The CPS License capacity for D+ Interface, calculated as shown below: [INT_ACC_CPS_DPLUS + INT_ACC_CPS_SIPE + INT_ACC_CPS_ENUME].	True	SUM
PEAK_CPS_LIC_DPLUS	GAUGE	No	Peak CPS usage for DPLUS Interface when CPS-based Licensing is enforced	True	AVG
PEAK_CPS_LIC_SIPE	GAUGE	No	Peak CPS usage for SIPE Interface when CPS-based Licensing is enforced	True	AVG
PEAK_CPS_LIC_ENUME	GAUGE	No	Peak CPS usage for ENUME Interface when CPS-based Licensing is enforced	True	AVG
ACC_CPS_LIC_SIPE_INVITE	COUNTER	No	Invite Calls Accepted for Sipe Interface with CPS-based Licensing enforced	True	SUM
ACC_CPS_LIC_SIPE_SUBSCRIBE	COUNTER	No	Subscribe Calls Accepted for Sipe Interface with CPS-based Licensing enforced	True	SUM
ACC_CPS_LIC_SIPE_NOTIFY	COUNTER	No	Notify Calls Accepted for Sipe Interface with CPS-based Licensing enforced	True	SUM
ACC_CPS_LIC_SIPE_REGISTER	COUNTER	No	Register Calls Accepted for Sipe Interface with CPS-based Licensing enforced	True	SUM
ACC_CPS_LIC_SIPE_OPTIONS	COUNTER	No	Options Calls Accepted for Sipe Interface with CPS-based Licensing enforced	True	SUM
ACC_CPS_LIC_SIPE_MESSAGE	COUNTER	No	Message Calls Accepted for Sipe Interface with CPS-based Licensing enforced	True	SUM
ACC_CPS_LIC_SIPE_REFER	COUNTER	No	Refer Calls Accepted for Sipe Interface with CPS-based Licensing enforced	True	SUM
ACC_CPS_LIC_SIPE_OTHERS	COUNTER	No	Others Calls Accepted for Sipe Interface with CPS-based Licensing enforced	True	SUM
LICENSE_MODE	GAUGE	No	License Mode of the node: 0 = Node Locked. 1 = Domain Locked	True	SUM

Column Name	Column Type	Index	Description	canAggregate	canAggregateType
PEAK_CPS_LIC_SIPE_INVITE	GAUGE	No	Invite Peak CPS usage for SIPE Interface when CPS-based Licensing is enforced	True	AVG
PEAK_CPS_LIC_SIPE_SUBSCRIBE	GAUGE	No	Subscribe Peak CPS usage for SIPE Interface when CPS-based Licensing is enforced	True	AVG
PEAK_CPS_LIC_SIPE_NOTIFY	GAUGE	No	Notify Peak CPS usage for SIPE Interface when CPS-based Licensing is enforced	True	AVG
PEAK_CPS_LIC_SIPE_REGISTER	GAUGE	No	Register Peak CPS usage for SIPE Interface when CPS-based Licensing is enforced	True	AVG
PEAK_CPS_LIC_SIPE_OPTIONS	GAUGE	No	Options Peak CPS usage for SIPE Interface when CPS-based Licensing is enforced	True	AVG
PEAK_CPS_LIC_SIPE_MESSAGE	GAUGE	No	Message Peak CPS usage for SIPE Interface when CPS-based Licensing is enforced	True	AVG
PEAK_CPS_LIC_SIPE_REFERER	GAUGE	No	Refer Peak CPS usage for SIPE Interface when CPS-based Licensing is enforced	True	AVG
PEAK_CPS_LIC_SIPE_OTHERS	GAUGE	No	Others Peak CPS usage for SIPE Interface when CPS-based Licensing is enforced	True	AVG
INT_ACC_CPS_LIC_SIPE_INVITE	INTEGER	No	The total number of invite Calls Accepted for Sipe Interface per second with CPS-based Licensing enforced	True	SUM
INT_ACC_CPS_LIC_SIPE_SUBSCRIBE	INTEGER	No	The total number of subscribe Calls Accepted for Sipe Interface per second with CPS-based Licensing enforced	True	SUM
INT_ACC_CPS_LIC_SIPE_NOTIFY	INTEGER	No	The total number of Notify Calls Accepted for Sipe Interface per second with CPS-based Licensing enforced	True	SUM
INT_ACC_CPS_LIC_SIPE_REGISTER	INTEGER	No	The total number of Register Calls Accepted for Sipe Interface per second with CPS-based Licensing enforced	True	SUM
INT_ACC_CPS_LIC_SIPE_OPTIONS	INTEGER	No	The total number of Options Calls Accepted for Sipe Interface per second with CPS-based Licensing enforced	True	SUM

Column Name	Column Type	Index	Description	canAggregate	canAggregateType
INT_ACC_CPS_LIC_SIPE_MESSAGE	INTEGER	No	The total number of Message Calls Accepted for Sipe Interface per second with CPS-based Licensing enforced	True	SUM
INT_ACC_CPS_LIC_SIPE_REFER	INTEGER	No	The total number of Refer Calls Accepted for Sipe Interface per second with CPS-based Licensing enforced	True	SUM
INT_ACC_CPS_LIC_SIPE_OTHERS	INTEGER	No	The total number of Others Calls Accepted for Sipe Interface per second with CPS-based Licensing enforced	True	SUM
CNE_ACCEPTED_CPS_DPLUS	COUNTER	No	The CNE Calls Accepted for D+ Interface with CPS-Based Licensing enforced.	True	SUM
CNE_ACCEPTED_CPS_SIPE	COUNTER	No	The CNE Calls Accepted for Sipe Interface with CPS-Based Licensing enforced.	True	SUM
CNE_ACCEPTED_CPS_ENUME	COUNTER	No	The CNE Calls Accepted for Enume Interface with CPS-Based Licensing enforced.	True	SUM
CNE_PEAK_CPS_DPLUS	GAUGE	No	The CNE Peak CPS usage for DPLUS Interface when CPS-Based Licensing is enforced.	True	Mean
CNE_PEAK_CPS_SIPE	GAUGE	No	The CNE Peak CPS usage for SIPE Interface when CPS-Based Licensing is enforced.	True	Mean
CNE_PEAK_CPS_ENUME	GAUGE	No	The CNE Peak CPS usage for ENUME Interface when CPS-Based Licensing is enforced.	True	Mean
BASE_CNE	INTEGER	No	The Base CNE.	True	SUM

PSXEscapeServices

PSXEscapeServiceStats

Column Name	Column Type	Index	Description	canAggregate
ESC_SERVICE_NAME	STRING	true	The name of the service that skipped the counters as the license is not available.	false

Column Name	Column Type	Index	Description	canAggregate
ESC_SERVICE_COUNT	COUNTER64	false	The number of times the service skipped.	true

PSXEscapeServiceStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
ESC_SERVICE_NAME	STRING	true	The name of the service that skipped the counters as the license is not available.	false	NA
ESC_SERVICE_COUNT	COUNTER64	false	The number of times the service skipped.	true	SUM

PSXHpc

PSXHpcCallStats

Column Name	Column Type	Index	Description
IP	IPADDRESS	Yes	The GSX IP address to which the HPC Calls counter applies
NAME	STRING	No	The GSX name to which the HPC Calls counters applies
INGRESS_PSTN	COUNTER	No	The number of HPC calls coming in from PSTN calls

PsxHpcGetsZoneStats

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
ZONE_NAME_LENGTH	INTEGER	Yes	Length of the Zone Name	False	NA
ZONE_NAME	VARCHAR2	Yes	Zone Name for which counters are applicable	False	NA

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
TRANSPORT_TYPE	INTEGER	Yes	The transport type used towards the Zone.1-tcp, 2-udp, 3-tcp fallback	False	NA
HPC_DNS_REQ	COUNTER	No	Number of HPC DNS requests sent for the Zone.	False	SUM
HPC_DNS_RES	COUNTER	No	Number of HPC DNS responses received for the Zone.	False	SUM
HPC_DNS_NO_ANS_RSP	COUNTER	No	Number of HPC DNS no answer responses received for the Zone.	False	SUM
HPC_DNS_TIMEOUT	COUNTER	No	Number of HPC DNS requests timed out for the Zone.	False	SUM
HPC_DNS_DEST_UNREACHABLE	COUNTER	No	Number of HPC DNS requests failed due to destination unreachable for the Zone.	False	SUM
NON_HPC_DNS_REQ	COUNTER	No	Number of Non HPC DNS requests sent for the Zone.	False	SUM
NON_HPC_DNS_RES	COUNTER	No	Number of Non HPC DNS responses received for the Zone.	False	SUM
NON_HPC_DNS_NO_ANS_RSP	COUNTER	No	Number of Non HPC DNS no answer responses received for the Zone.	False	SUM
NON_HPC_DNS_TIMEOUT	COUNTER	No	Number of Non HPC DNS requests timed out for the Zone.	False	SUM
NON_HPC_DNS_DEST_UNREACHABLE	COUNTER	No	Number of Non HPC DNS requests failed due to destination unreachable for the Zone.	False	SUM

PSXHPCGetsCounterStats

Column Name	Column Type	Index	Description	canAggregate
HPC_TOTAL_COUNT	INTEGER	No	Count of Total HPC calls	False
NON_HPC_TOTAL_COUNT	INTEGER	No	Count of Total non-HPC calls	False
HPC_FAILURE_COUNT	INTEGER	No	Count of Total HPC calls Failed	False
NON_HPC_FAILURE_COUNT	INTEGER	No	Count of Total Non-HPC calls failed	False

PsxHpcGetsServerStats

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SERVER_IP_ADDRESS_TYPE	INTEGER	True	The ENUM/DNS Server IP address Type.	True	Mean
SERVER_IP_ADDRESS	STRING	True	The ENUM/DNS Server IP address.	False	
SERVER_PORT	INTEGER	True	The Port on which ENUM/DNS server is listening.	True	Mean
SERVER_TRANSPORT_TYPE	INTEGER	True	The transport storageDataType used towards the ENUM/DNS Server.1-tcp, 2-udp, 3-tcp fallback.	True	Mean
HPC_DNS_REQ	COUNTER	False	Number of DNS requests sent to the server for High Priority Calls.	True	Sum
HPC_DNS_RES	COUNTER	False	Number of DNS responses received from the Server for High Priority Calls.	True	Sum

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
HPC_DNS_NO_ANS_RSP	COUNTER	False	Number of DNS no answer responses received from the Server for High Priority Calls.	True	Sum
HPC_DNS_TIMEOUT	COUNTER	False	Number of HPC DNS requests timed out for the Server.	True	Sum
HPC_DNS_DEST_UNREACHABLE	COUNTER	False	Number of HPC DNS requests failed due to destination unreachable for the Server.	True	Sum
NON_HPC_DNS_REQ	COUNTER	False	Number of DNS requests sent to the Server for Non High Priority Calls.	True	Sum
NON_HPC_DNS_RES	COUNTER	False	Number of DNS responses received from the Server for Non High Priority Calls.	True	Sum
NON_HPC_DNS_NO_ANS_RSP	COUNTER	False	Number of DNS no answer responses received from the Server for Non High Priority Calls.	True	Sum
NON_HPC_DNS_TIMEOUT	COUNTER	False	Number of Non HPC DNS requests timed out for the Server.	True	Sum
NON_HPC_DNS_DEST_UNREACHABLE	COUNTER	False	Number of Non HPC DNS requests failed due to destination unreachable for the Server.	True	Sum

PSXHpcSipeReqRecvStats

Column Name	Column Type	Index	Description	canAggregate
REQ_RECV_SUBS_ETS_RPH	COUNTER	No	Tracks the number of SUBSCRIBE requests with ETS RPH received by the SIP process	false
REQ_RECV_SUBS_ETS_DN	COUNTER	No	Tracks the number of SUBSCRIBE requests with ETS DN received by the SIP process	false
SUBREQ_WITH_ETS_RPH_DIS_OL	COUNTER	No	Tracks the number of SUBSCRIBE requests with ETS RPH discarded due to overload	false
SUBREQ_WITHOUT_ETS_RPH_DIS_OL	COUNTER	No	Tracks the number of SUBSCRIBE requests without ETS RPH discarded due to overload	false
REQ_RECV_NOTIFY_ETS_RPH	COUNTER	No	Tracks the number of Notify requests with ETS RPH received by the SIP process	false
REQ_RECV_NOTIFY_ETS_DN	COUNTER	No	Tracks the number of Notify requests with ETS DN received by the SIP process	false
NOTREQ_WITH_ETS_RPH_DIS_OL	COUNTER	No	Tracks the number of Notify requests with ETS RPH discarded due to overload	false
NOTREQ_WITHOUT_ETS_RPH_DIS_OL	COUNTER	No	Tracks the number of Notify requests without ETS RPH discarded due to overload	false
REQ_RECV_REG_ETS_RPH	COUNTER	No	Tracks the number of REGISTER requests with ETS RPH received by the SIP process	false
REQ_RECV_REG_ETS_DN	COUNTER	No	Tracks the number of REGISTER requests with ETS DN but no ETS RPH received by the SIP process	false

Column Name	Column Type	Index	Description	canAggregate
REGREQ_WITH_ETS_RPH_DIS_OL	COUNTER	No	Tracks the number of REGISTER Requests with ETS RPH discarded due to overload	false
REGREQ_WITHOUT_ETS_RPH_DIS_OL	COUNTER	No	Tracks the number of REGISTER Requests without ETS RPH discarded due to overload	false
REQ_RECV_OPT_ETS_RPH	COUNTER	No	Tracks the number of OPTIONS requests with ETS RPH, received by the SIP process	false
REQ_RECV_OPT_ETS_DN	COUNTER	No	Tracks the number of OPTIONS requests with ETS DN but no ETS RPH received by the SIP process Retransmissions of messages are not counted	false
OPTREQ_WITH_ETS_RPH_DIS_OL	COUNTER	No	Tracks the number of OPTIONS Requests with ETS RPH discarded due to overload	false
OPTREQ_WITHOUT_ETS_RPH_DIS_OL	COUNTER	No	Tracks the number of OPTIONS Requests without ETS RPH discarded due to overload	false
REQ_RECV_MES_ETS_RPH	COUNTER	No	Tracks the number of MESSAGE requests with ETS RPH received by the SIP process	false
REQ_RECV_MES_ETS_DN	COUNTER	No	Tracks the number of MESSAGE requests with ETS DN but no ETS RPH received by the SIP process	false
MESREQ_WITH_ETS_RPH_DIS_OL	COUNTER	No	Tracks the number of MESSAGE Requests with ETS RPH discarded due to overload	false
MESREQ_WITHOUT_ETS_RPH_DIS_OL	COUNTER	No	Tracks the number of MESSAGE Requests without ETS RPH discarded due to overload	false

Column Name	Column Type	Index	Description	canAggregate
REQ_RECV_REF_ET S_RPH	COUNTER	No	Tracks the number of REFER requests with ETS RPH, received by the SIP process	false
REQ_RECV_REF_ET S_DN	COUNTER	No	Tracks the number of REFER requests with ETS DN but no ETS RPH received by the SIP process	false
REFREQ_WITH_ET S_RPH_DIS_OL	COUNTER	No	Tracks the number of REFER Requests with ETS RPH discarded due to overload	false
REFREQ_WITHOUT_ ETS_RPH_DIS_OL	COUNTER	No	Tracks the number of REFER Requests without ETS RPH discarded due to overload	false

PSXHpcSipeRespSentStats

Column Name	Column Type	Index	Description	canAggregate
RSP_SENT_SUB_ET S_RPH	COUNTER	No	Tracks the number of Subscribe requests sent with ETS RPH	false
RSP_SENT_NOTIFY_ ETS_RPH	COUNTER	No	Tracks the number of Notify requests sent with ETS RPH	false
RSP_SENT_REGISTE R_ET S_RPH	COUNTER	No	Tracks the number of Register requests sent with ETS RPH	false
RSP_SENT_OPTION_ ETS_RPH	COUNTER	No	Tracks the number of Option requests sent with ETS RPH	false
RSP_SENT_MESSAG E_ET S_RPH	COUNTER	No	Tracks the number of Message requests sent with ETS RPH	false
RSP_SENT_REFER_ ETS_RPH	COUNTER	No	Tracks the number of REFER requests sent with ETS RPH	false

PSXHTTP**PsxHTTPCounterStats**

Column Name	Column Type	Index	Description
HTTPC_SIGN_REQ_CTRS	COUNTER	False	Count of Signing Service Requests.
HTTPC_SIGN_RES_CTRS	COUNTER	False	Count of Signing Service Responses.
HTTPC_SIGN_TIMEOUT_CTRS	COUNTER	False	Count of Signing Service Timeout.
HTTPC_SIGN_MISS_PARAM_CTRS	COUNTER	False	Count of Signing Service failure due to Missing Mandatory Parameters.
HTTPC_SIGN_VER_REQ_CTRS	COUNTER	False	Count of Verification Service Request.
HTTPC_SIGN_VER_RES_CTRS	COUNTER	False	Count of Verification Service Response.
HTTPC_SIGN_VER_TIMEOUT_CTRS	COUNTER	False	Count of Verification Service TimeOut.
HTTPC_SIGN_VER_MIS_PARAM_CTRS	COUNTER	False	Count of Verification Service failure due to Missing Mandatory Parameters.
HTTPC_SIGN_TAG_MIS_PARAM_CTRS	COUNTER	False	Count of Tagging Service failure due to Missing Mandatory Parameters.
HTTPC_REST_TREQ_CTRS	COUNTER	False	Count of Signing Service Requests.
HTTPC_REST_RESP_CTRS	COUNTER	False	Count of Signing Service Responses.
HTTPC_REST_TIMEOUT_CTRS	COUNTER	False	Count of Signing Service Timeout.
HTTPC_REST_PARAM_CTRS	COUNTER	False	Count of Signing Service failure due to Missing Mandatory Parameters.
HTTPC_REST_RESP_PARAM_CTRS	COUNTER	False	Count of Verification Service Request.

Column Name	Column Type	Index	Description
HTTPC_MULTI_STI_SERVICE_EXEC_CTRS	COUNTER	False	Count of calls for which multiple STI Services are run.

PsxHttpClientInternalStats

Column Name	Column Type	Index	Description
NO_CONN_AVAILABLE_CTRS	COUNTER	False	Keeps track of the number of errors with no connection available
HTTP_SIGN_RES_IDENTITY_HDR_SIZEOUT NOTE: Available only for PSX 15.1.2	COUNTER	False	Keeps track of the number of Identity Header dropped due to size limit in signing response.
HTTP_JSON_ERROR_CTRS	COUNTER	False	Keeps track of the number of JSON Errors
HTTP_CURL_ERROR_CTRS	COUNTER	False	Keeps track of the number of HTTP Errors
HTTP_MAX_RETRY_EXHAUST_CTRS	COUNTER	False	Keeps track of the number of failures due to Max Retries Exhausted
HTTP_GENERAL_FAIL_CTRS	COUNTER	False	Keeps track of the number of General Failure
HTTP_JSON_ERROR_CTRS_REQ	COUNTER	False	Keeps track of the number of the number of JSON Errors in Request Schema which have been received by the http process counted for each FQDN

PSXHTTPClientRESTServiceCountersStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
HTTP_REST_QUERY_SENT	COUNTER	False	Tracks the number of REST Service requests which are sent from HTTP Client Process.	True	SUM	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
HTTP_REST_RSP	COUNTER	False	Tracks the number of REST Service responses received by HTTP Client process.	True	SUM	Yes
HTTP_REST_QUERY_TIMEOUT	COUNTER	False	Tracks the number of REST Service requests which have timeout for response.	True	SUM	Yes
HTTP_REST_QUERY_RETRY	COUNTER	False	Tracks the number of REST Service requests which are retried from HTTP Client Process.	True	SUM	Yes

PSXHTTPClientRESTServiceFailureCountersStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
HTTP_REST_FAILURE_400_COUNTERS	COUNTER	False	Tracks the number of 400 error received from REST Service server.	True	SUM	Yes
HTTP_REST_FAILURE_403_COUNTERS	COUNTER	False	Tracks the number of 403 error received from REST Service server.	True	SUM	Yes
HTTP_REST_FAILURE_500_COUNTERS	COUNTER	False	Tracks the number of 500 error received from REST Service server.	True	SUM	Yes
HTTP_REST_FAILURE_503_COUNTERS	COUNTER	False	Tracks the number of 503 error received from REST Service server.	True	SUM	Yes

PSXHttpPerlStats

Column Name	Column type	Index	Description	CanAggregate
IP_ADDRESS_TYPE	INTEGER	Yes	Server IP address type.	False
IP_ADDRESS	STRING	Yes	IP address of the STIR Server.	False
PORT	INTEGER	Yes	Port on which the server is listening.	False
MAX_CONNECTION_TIME	GAUGE	No	Tracks the maximum time taken to establish a connection.	False
MIN_CONNECTION_TIME	GAUGE	No	Tracks the minimum time taken to establish a connection.	False
AVG_CONNECTION_TIME	GAUGE	No	Tracks the average time taken to establish a connection.	False
MAX_RESPONSE_TIME	GAUGE	No	Tracks the maximum time taken for the server response.	False
MIN_RESPONSE_TIME	GAUGE	No	Tracks the minimum time taken for the server response	False
AVG_RESPONSE_TIME	GAUGE	No	Tracks the average time taken for the server response	False

PSXHTTPPerSvrTypeFailureCountersStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_FAIL_SERVER_NAME	STRING	True	Server Type Name.	false	N/A	Yes
HTTP_SIGN_FAILURE_E3	COUNTER	False	Tracks the number of E3 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_X1	COUNTER	False	Tracks the number of X1 error received from signing server per server type.	True	SUM	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_FAILURE_X2	COUNTER	False	Tracks the number of X2 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_X3	COUNTER	False	Tracks the number of X3 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_X4	COUNTER	False	Tracks the number of X4 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_400	COUNTER	False	Tracks the number of 400 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_404	COUNTER	False	Tracks the number of 404 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_405	COUNTER	False	Tracks the number of 405 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_406	COUNTER	False	Tracks the number of 406 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_411	COUNTER	False	Tracks the number of 411 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_415	COUNTER	False	Tracks the number of 415 error received from signing server per server type.	True	SUM	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_FAILURE_500	COUNTER	False	Tracks the number of 500 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_503	COUNTER	False	Tracks the number of 503 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_SVC_4000	COUNTER	False	Tracks the number of service exception 4000 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_SVC_4001	COUNTER	False	Tracks the number of service exception 4001 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_SVC_4002	COUNTER	False	Tracks the number of service exception 4002 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_SVC_4003	COUNTER	False	Tracks the number of service exception 4003 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_SVC_4004	COUNTER	False	Tracks the number of service exception 4004 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_SVC_4005	COUNTER	False	Tracks the number of service exception 4005 error received from signing server per server type.	True	SUM	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_FAILURE_SVC_4006	COUNTER	False	Tracks the number of service exception 4006 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_SVC_4007	COUNTER	False	Tracks the number of service exception 4007 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_POL_4050	COUNTER	False	Tracks the number of policy exception 4050 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_POL_5000	COUNTER	False	Tracks the number of policy exception 5000 error received from signing server per server type.	True	SUM	Yes
HTTP_FAILURE_E3	COUNTER	False	Tracks the number of E3 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E4	COUNTER	False	Tracks the number of E4 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E5	COUNTER	False	Tracks the number of E5 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E6	COUNTER	False	Tracks the number of E6 error received from verification server per server type.	True	SUM	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_FAILURE_E7	COUNTER	False	Tracks the number of E7 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E8	COUNTER	False	Tracks the number of E8 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E9	COUNTER	False	Tracks the number of E9 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E10	COUNTER	False	Tracks the number of E10 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E11	COUNTER	False	Tracks the number of E11 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E12	COUNTER	False	Tracks the number of E12 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E13	COUNTER	False	Tracks the number of E13 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E14	COUNTER	False	Tracks the number of E14 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E15	COUNTER	False	Tracks the number of E15 error received from verification server per server type.	True	SUM	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_FAILURE_E16	COUNTER	False	Tracks the number of E16 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E17	COUNTER	False	Tracks the number of E17 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E18	COUNTER	False	Tracks the number of E18 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E19	COUNTER	False	Tracks the number of E19 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E20	COUNTER	False	Tracks the number of E20 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E21	COUNTER	False	Tracks the number of E21 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E22	COUNTER	False	Tracks the number of E22 error received from verification server per server type.	True	SUM	Yes
HTTP_FAILURE_E23	COUNTER	False	Tracks the number of E23 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_X1	COUNTER	False	Tracks the number of X1 error received from verification server per server type.	True	SUM	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_VER_FAILURE_X2	COUNTER	False	Tracks the number of X2 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_X3	COUNTER	False	Tracks the number of X3 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_X4	COUNTER	False	Tracks the number of X4 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_400	COUNTER	False	Tracks the number of 400 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_404	COUNTER	False	Tracks the number of 404 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_405	COUNTER	False	Tracks the number of 405 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_406	COUNTER	False	Tracks the number of 406 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_411	COUNTER	False	Tracks the number of 411 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_415	COUNTER	False	Tracks the number of 415 error received from verification server per server type.	True	SUM	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_VER_FAILURE_500	COUNTER	False	Tracks the number of 500 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_503	COUNTER	False	Tracks the number of 503 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_SVC_4000	COUNTER	False	Tracks the number of service exception 4000 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_SVC_4001	COUNTER	False	Tracks the number of service exception 4001 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_SVC_4002	COUNTER	False	Tracks the number of service exception 4002 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_SVC_4003	COUNTER	False	Tracks the number of service exception 4003 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_SVC_4004	COUNTER	False	Tracks the number of service exception 4004 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_SVC_4005	COUNTER	False	Tracks the number of service exception 4005 error received from verification server per server type.	True	SUM	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_VER_FAILURE_SVC_4006	COUNTER	False	Tracks the number of service exception 4006 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_SVC_4007	COUNTER	False	Tracks the number of service exception 4007 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_POL_4050	COUNTER	False	Tracks the number of service exception 4050 error received from verification server per server type.	True	SUM	Yes
HTTP_VER_FAILURE_POL_5000	COUNTER	False	Tracks the number of service exception 5000 error received from verification server per server type.	True	SUM	Yes

PSXHTTPPerSvrTypeInternalCountersStats

Column Name	Column type	Index	Description	CanAggregate	Aggregation Formula	present in reports
HTTP_SIGNATURES_IDENTITY_HDR_SIZEOUT NOTE: Available only for PSX 15.1.2	COUNTER	False	Keeps track of the number of Identity Header dropped due to size limit in signing response Per Server Type.	-	SUM	-
HTTP_INTERNAL_SERVER_NAME	STRING	True	Server Type Name.	False	N/A	Yes

Column Name	Column type	Index	Description	CanAggregate	Aggregation Formula	present in reports
HTTP_NO_CONNECTION	COUNTER	False	Tracks the number of the errors with no connection available Per Server Type.	True	SUM	Yes
HTTP_JSON_ERROR	COUNTER	False	Tracks the number of JSON Error Per Server Type.	True	SUM	Yes
HTTP_CURL_ERROR	COUNTER	False	Tracks the number of HTTP Error Per Server Type.	True	SUM	Yes
HTTP_MAX_RETRY	COUNTER	False	Tracks the number of failures due to Max Retries Exhausted Per Server Type.	True	SUM	Yes
HTTP_GENERAL_FAILURE	COUNTER	False	Tracks the number of General Failure Per Server Type.	True	SUM	Yes
JSON_ERROR_REQUEST	COUNTER	False	Tracks the number of JSON Error Per Server Type for Request.	True	SUM	Yes

PSXHTTPPerSvrTypeSignVerCountersStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_SIGN_VER_NAME	STRING	True	Server Type Name	False	N/A	Yes
REQ_SENT	COUNTER	False	Tracks the number of Signing requests sent from HTTP Client Process Per Server Type.	True	SUM	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_RSP	COUNTER	False	Tracks the number of Signing responses received by HTTP Client process Per Server Type.	True	SUM	Yes
HTTP_INVALID_INP	COUNTER	False	Tracks the number of signing requests which failed due to invalid input Per Server Type.	True	SUM	Yes
HTTP_TIMEOUT	COUNTER	False	Tracks the number of signing requests which have timeout for response Per Server Type.	True	SUM	Yes
HTTP_RETRY	COUNTER	False	Tracks the number of Signing requests which are retried from HTTP Client Process Per Server Type.	True	SUM	Yes
HTTP_SENT	COUNTER	False	Tracks the number of Verification requests which are sent from HTTP Client Process.	True	SUM	Yes
HTTP_VERIFICATION_RSP	COUNTER	False	Tracks the number of Verification responses received by HTTP Client process.	True	SUM	Yes
HTTP_VER_INVALID_INP	COUNTER	False	Tracks the number of Verification requests which failed due to invalid input.	True	SUM	Yes
HTTP_VER_TIMEOUT	COUNTER	False	Tracks the number of Verification requests which have timeout for response.	True	SUM	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
HTTP_VER_QUERY_RETRY	COUNTER	False	Tracks the number of Verification requests which are retried from HTTP Client Process.	True	SUM	Yes

PSXHttpSigningFailStats

Column Name	Column Type	Index	Description	canAggregate
SIGNING_FAILURE_E3	COUNTER	False	Keeps track of the number of E3 error received from signing server	False
SIGNING_FAILURE_X1	COUNTER	False	Keeps track of the number of X1 error received from signing server.	False
SIGNING_FAILURE_X2	COUNTER	False	Keeps track of the number of X2 error received from signing server.	False
SIGNING_FAILURE_X3	COUNTER	False	Keeps track of the number of X3 error received from signing server	False
SIGNING_FAILURE_X4	COUNTER	False	Keeps track of the number of X4 error received from signing server.	False
SIGNING_FAILURE_400	COUNTER	False	Keeps track of the number of 400 error received from signing server.	False
SIGNING_FAILURE_404	COUNTER	false	Tracks the number of 404 error received from signing server.	false
SIGNING_FAILURE_405	COUNTER	false	Tracks the number of 405 error received from signing server.	false
SIGNING_FAILURE_406	COUNTER	false	Tracks the number of 406 error received from signing server.	false

Column Name	Column Type	Index	Description	canAggregate
SIGNING_FAILURE 411	COUNTER	false	Tracks the number of 411 error received from signing server.	false
SIGNING_FAILURE 415	COUNTER	false	Tracks the number of 415 error received from signing server.	false
SIGNING_FAILURE 500	COUNTER	False	Keeps track of the number of 500 error received from signing server.	False
SIGNING_FAILURE 503	COUNTER	False	Keeps track of the number of 503 error received from signing server.	False
SIGNING_FAILURE SVC4000	COUNTER	false	Tracks the number of service exception 4001 error received from the signing server.	false
SIGNING_FAILURE SVC4001	COUNTER	false	Tracks the number of service exception 4001 error received from the signing server.	false
SIGNING_FAILURE SVC4002	COUNTER	false	Tracks the number of service exception 4002 error received from the signing server.	false
SIGNING_FAILURE SVC4003	COUNTER	false	Tracks the number of service exception 4003 error received from the signing server.	false
SIGNING_FAILURE SVC4004	COUNTER	false	Tracks the number of service exception 4004 error received from the signing server.	false
SIGNING_FAILURE SVC4006	COUNTER	false	Tracks the number of service exception 4006 error received from the signing server.	false
SIGNING_FAILURE SVC4007	COUNTER	false	Tracks the number of service exception 4007 error received from the signing server.	false
SIGNING_FAILURE POL4050	COUNTER	false	Tracks the number of policy exception 4050 error received from the signing server. oid: .1.3.6.1.4.1.	false

Column Name	Column Type	Index	Description	canAggregate
SIGNING_FAILURE_POL5000	COUNTER	false	Tracks the number of policy exception 5000 error received from the signing server.	false

PSXHttpSigningStats

Column Name	Column Type	Index	Description	canAggregate
SIGNING_QUERY_SENT	COUNTER	False	Keeps track of the number of Signing requests which are sent from HTTP Client Process.	False
SIGNING_RSP	COUNTER	False	Keeps track of the number of Signing responses received by HTTP Client process.	False
SIGNING_INVALID_INPUT	COUNTER	False	Keeps track of the number of signing requests which failed due to invalid input	False
SIGNING_QUERY_TIMEOUT	COUNTER	False	Keeps track of the number of signing requests which have timeout for response	False
SIGNING_QUERY_RETRY_COUNT	COUNTER	FALSE	Tracks the number of Signing Query retries sent from the HTTP Client Process	TRUE
SIGNING_QUERY_SENT_CPS	COUNTER	FALSE	This counter calculates the CPS of the Signing Queries sent from the HTTP Client Process (CPS = Delta from previous interval / interval size)	TRUE

PSXHttpVerificationStats

Column Name	Column Type	Index	Description	canAggregate
VERIFICATION_QUERY_SENT	COUNTER	False	Keeps track of the number of Verification requests which are sent from HTTP client Process.	False

Column Name	Column Type	Index	Description	canAggregate
VERIFICATION_RSP	COUNTER	False	Keeps track of the number of Verification responses received by HTTP client process.	False
VERIFICATION_INVALID_INPUT	COUNTER	False	Keeps track of the number of Verification requests which failed due to invalid input.	False
VERIFICATION_QUERY_TIMEOUT	COUNTER	False	Keeps track of the number of Verification requests which have timeout for response.	False
VERIFICATION_QUERY_RETRY_COUNT	COUNTER	FALSE	Tracks the number of Verification Query Retries sent from the HTTP Client Process	TRUE
VERIFICATION_QUERY_SENT_CPS	COUNTER	FALSE	This counter calculates the CPS of Verification Queries sent from the HTTP Client Process (CPS = Delta from previous interval / interval size)	TRUE

PSXInd

PSXINDCALLSVCTYPESIPSERVERSIPSTATS

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
SIP_SERVER	STRING	True	SIP server	False	N/A	Yes
CALL_SVC_TYPE	STRING	True	Call service type	False	N/A	Yes
SVC_TYPE_COUNTER	COUNTER	False	Total calls received with this service type	False	SUM	Yes

PSXIndSIPServerSIPStats

Note

The performance statistics file is generated only if statistics collection is enabled and the count is not zero. That is actual calls are made.

For more information, refer to [PSX Statistics Collection Based on SIP Server](#).

Column Name	Column Type	Index	Description	canAggregate
SIP_SERVER	STRING	True	Name of the SIP Server.	False
SIP_METHOD	STRING	True	SIP Method.	False
REC_SENT	STRING	True	Records Sent/Received.	False
CODE_ID	GAUGE	True	SIP Code ID.	False
COUNTER	COUNTER	False	Counter indicating how many times SIP CODE was observed.	True

PSXIndividualPSXSIPStats**Note**

The performance statistics file is generated only if statistics collection is enabled and the count is not zero. That is actual calls are made.

For more information, refer to [PSX Statistics Collection Based on SIP Server](#).

Column Name	Column Type	Index	Description	canAggregate
CODE_ID	GAUGE	True	SIP Code ID.	False
COUNTER	COUNTER	False	Counter indicating how many times SIP CODE was observed.	True
REC_SENT	STRING	True	Records Sent/Received.	False
SIP_METHOD	STRING	True	SIP Method.	False

PSXLnpPerSipServerCountersStats

Column Name	Column Type	Index	Description	canAggregate
SIP_SERVER_NAME	STRING	true	The SIP server name.	false
LNPREQ_RCVD	COUNTER	false	Tracks the number of LNP requests.	true
LNPREQ_LRNRS P	COUNTER	false	Tracks the number of responses contain Location Routing Number (LRN) .	true
LNPREQ_WO_LRNRS P	COUNTER	false	Tracks the number of responses do not contain LRN.	true
CT_RCVD	COUNTER	false	Tracks the number of requests contain QTYPE as class.	true
CT_SUCCESS	COUNTER	false	Tracks the number of successful queries for QTYPE class.	true
CT_FAILED	COUNTER	false	Tracks the number of failed queries for QTYPE class.	true
LIDB_TYPE_RCVD	COUNTER	false	Tracks the number of requests contain QTYPE as Line Identity Database (LIDB) .	true
LIDB_TYPE_SUCCESS	COUNTER	false	Tracks the number of successful queries for QTYPE LIDB.	true
LIDB_TYPE_FAILED	COUNTER	false	Tracks the number of failed queries for QTYPE LIDB.	true
CNAM_TYPE_RCVD	COUNTER	false	Tracks the number of requests contain QTYPE as Calling Name (CNAM) .	true
CNAM_TYPE_SUCCESS	COUNTER	false	Tracks the number of successful queries for QTYPE CNAM.	true
CNAM_TYPE_FAILED	COUNTER	false	Tracks the number of failed queries for QTYPE CNAM.	true
ISVM_TYPE_RCVD	COUNTER	false	Tracks the number of requests contain QTYPE as Inter-Switch Voice Mail (ISVM) .	true

Column Name	Column Type	Index	Description	canAggregate
ISVM_TYPE_SUCCESS	COUNTER	false	Tracks the number of successful queries for QTYPE ISVM.	true
ISVM_TYPE_FAILED	COUNTER	false	Tracks the number of failed queries for QTYPE ISVM.	true

PSXNumCallsRecordedCRCStats

Column Name	Column Type	Index	Description
CRITERIA_NAME	STRING	Yes	The Criteria Name that the Num Call recorded counter apply to.
NUM_CALLS	COUNTER	No	The Number of calls recorded for the criteria.

PSXOutgoingLicStats

Column Name	Column Type	Index	Description	canAggregate
FEATURE_NAME	STRING	True	FeatureId (or SKU) for which usage limit is specified	False
USAGE	INTEGER	False	Provisioned total BASE Count for the license on the node	False

PSXPeerOverloadThrottlingStats

Column Name	Column Type	Index	Description
IP_ADDRESS_TYPE	INTEGER	Yes	SIP PEER Host's IP address Type.
IP_ADDRESS	STRING	Yes	The IP address of the Peer for which throttling is performed
PORT	INTEGER	Yes	The Port on which Peer is listening when throttling is performed.

Column Name	Column Type	Index	Description
TANSPORT_TYPE	INTEGER	Yes	The transport used towards the Peer for which throttling is performed.1-tcp,2-udp and 3-sctp.
REQ_RCVD	COUNTER	No	Keeps track of no. of requests received for the Peer being throttled.
REQ_SENT	COUNTER	No	Keeps track of no. of requests sent to the Peer that is being throttled.
REQ_REJ	COUNTER	No	Keeps track of no. of requests rejected for the Peer that is being throttled.
REJ_RCVD	COUNTER	No	Keeps track of no. of rejects received from Peer that is being throttled.

PsxPerFqdnCounterStats

Column Name	Column Type	Index	Description	canAggregate
FQDN_NAME	STRING	true	FQDN name.	false
REQ_SENT	COUNTER	false	Tracks the number of requests sent by the FQDN.	false
RES_RECV	COUNTER	false	Tracks the number of responses received by the FQDN.	false
RES400_RECV	COUNTER	false	Tracks the number of 400 responses received by the FQDN.	false
RES500_RECV	COUNTER	false	Tracks the number of 500 responses received by the FQDN.	false
RES503_RECV	COUNTER	false	Tracks the number of 503 responses received by the FQDN.	false
TIMEOUTS	COUNTER	false	Tracks the number of Timeouts.	false
NO_CONN_AVAILABLE	COUNTER	false	Tracks the number of No Connections Available.	false
JSON_ERR	COUNTER	false	Tracks the number of JSON Error.	false

Column Name	Column Type	Index	Description	canAggregate
HTTP_ERR	COUNTER	false	Tracks the number of HTTP Error.	false
MAX_RETRY_EX	COUNTER	false	Tracks the number of Failures due to Max Retry Exhausted.	false
GEN_FAIL	COUNTER	false	Tracks the number of General Failures.	false
403_RECVD	COUNTER	false	Tracks the number of 403 responses received by the http process counted for each FQDN.	true
JSON_ERR_REQ	COUNTER	false	Tracks the number of JSON Errors in Request Schema which have been received by the http process counted for each FQDN.	false

PSXPes

PSXPesCallServiceTypeStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Report
SERVICE_TYPE	STRING	True	Key1 call service type	False	N/A	Yes
SVC_COUNTER_RCV	COUNTER	False	Total calls received with this service type	False	SUM	Yes

PSXPesCapCountersStats

Column Name	Column Type	Index	Description
SK_VALUE	INTEGER	Yes	Key1: Service Key
SERVICE_TYPE_VALUE	INTEGER	Yes	Key2: Service Type

Column Name	Column Type	Index	Description
NUM_IDP_SENT	COUNTER	No	Number of CAP Initial DP messages sent by the PSX
NUM_CON_RCVD	COUNTER	No	Number of CAMEL Connect messages received
NUM_CUE_CWA_RCVD	COUNTER	No	Number of CAP Continue and Continue with Argument messages received
NUM_ETC_RCVD	COUNTER	No	Number of CAP ETC messages received
NUM_CAP_REL_RCVD	COUNTER	No	Number of CAP RELEASE messages received
NUM_SSF_ERR	COUNTER	No	Number of CAP Errors messages From SSF to SCF
NUM_SCF_ERR	COUNTER	No	Number of CAP Errors messages From SCF to SSF
NUM_CAP_ARI_SENT	COUNTER	No	Number of CAP ARI messages Sent by the PSX
NUM_CAP_CTR_RCVD	COUNTER	No	Number of CAP CTR messages received

PSXPesDscNpCountersStats

Column Name	Column Type	Index	Description	canAggregate
REQUEST_VALUE	COUNTER	False	The total number of DSC originated NP requests received by the PSX.	True
SUCCESS_VALUE	COUNTER	False	The total number of DSC NP responses where the status was set to Success (this includes Ported, Not Ported, and Predipped).	True

Column Name	Column Type	Index	Description	canAggregate
PORTED_VALUE	COUNTER	False	The total number of DSC NP requests (calls) that resulted in a ported number with an Location Routing Number (LRN). The total number of calls where the number portability lookup is performed, and the result is ported with an LRN.	True
NOT_PORTED_VALUE	COUNTER	False	The total number of DSC NP requests (calls) where the number portability lookup is performed, and the result is not ported with no LRN.	True
PREDIPPED_VALUE	COUNTER	False	The total number of DSC NP requests (calls) where the number portability lookup is performed but the Policy Request already included LNP information (for example, FCI M-bit was set and LRN was received).	True
FAILURE_VALUE	COUNTER	False	The total number of DSC NP responses (calls) where the status was set to Failure. It is possible that the number portability lookup was performed, but the result is a failure due to some other PES processing.	True

PSXPesEnumSrcNumberCountersStats

Column Name	Column Type	Index	Description	Aggregation Type
PES_ENUM_REQ_CALLING	COUNTER	False	Number of ENUM requests received for the Calling number.	SUM
PES_ENUM_RSP_CALLING	COUNTER	False	Total number of ENUM responses for Calling Number.	SUM
PES_ENUM_RSP_CALLING_SUCCESS	COUNTER	False	Number of Successful ENUM responses for Calling number.	SUM

Column Name	Column Type	Index	Description	Aggregation Type
PES_ENUM_RSP_CALLING_GENERAL_FAILURE	COUNTER	False	Number of ENUM responses with General Failure for Calling number.	SUM
PES_ENUM_RSP_CALLING_INVALID	COUNTER	False	Number of ENUM responses with Invalid_Parameter Failure for Calling number.	SUM
PES_ENUM_RSP_CALLING_NO_DATA	COUNTER	False	Number of ENUM responses with Valid_Name_But_No_Data_Record Failure for Calling number.	SUM
PES_ENUM_RSP_CALLING_NO_MEM	COUNTER	False	Number of ENUM responses with Memory_Unavailable Failure for Calling number.	SUM
PES_ENUM_RSP_CALLING_NO_NAME	COUNTER	False	Number of ENUM responses with Name_Does_Not_Exist Failure for Calling number.	SUM
PES_ENUM_REQ_CALLED	COUNTER	False	Number of ENUM requests received for Called number.	SUM
PES_ENUM_RSP_CALLED	COUNTER	False	Total number of ENUM responses for Called Number.	SUM
PES_ENUM_RSP_CALLED_SUCCESS	COUNTER	False	Number of Successful ENUM responses for Called number.	SUM
PES_ENUM_RSP_CALLED_GENERAL_FAILURE	COUNTER	False	Number of ENUM responses with General Failure for Called number.	SUM
PES_ENUM_RSP_CALLED_INVALID	COUNTER	False	Number of ENUM responses with Invalid_Parameter Failure for Called number.	SUM
PES_ENUM_RSP_CALLED_NO_DATA	COUNTER	False	Number of ENUM responses with Valid_Name_But_No_Data_Record Failure for Called number.	SUM

Column Name	Column Type	Index	Description	Aggregation Type
PES_ENUM_RSP_CALLED_NO_MEM	COUNTER	False	Number of ENUM responses with Memory_Unavailable Failure for Called number.	SUM
PES_ENUM_RSP_CALLED_NO_NAME	COUNTER	False	Number of ENUM responses with Name_Does_Not_Exist Failure for Called number.	SUM
PES_ENUM_REQ_DIALED_ONLY	COUNTER	False	Number of ENUM requests received for Dialed Only number.	SUM
PES_ENUM_RSP_DIALED_ONLY	COUNTER	False	Total number of ENUM responses for Dialed Only Number.	SUM
PES_ENUM_RSP_DIALED_ONLY_SUCCESS	COUNTER	False	Number of Successful ENUM responses for Dialed Only number.	SUM
PES_ENUM_RSP_DIALED_ONLY_GENERAL_FAILURE	COUNTER	False	Number of ENUM responses with General Failure for Dialed Only number.	SUM
PES_ENUM_RSP_DIALED_ONLY_INVALID	COUNTER	False	Number of ENUM responses with Invalid_Parameter Failure for Dialed Only number.	SUM
PES_ENUM_RSP_DIALED_ONLY_NO_DATA	COUNTER	False	Number of ENUM responses with Valid_Name_But_No_Data_Record Failure for Dialed Only number.	SUM
PES_ENUM_RSP_DIALED_ONLY_NO_MEM	COUNTER	False	Number of ENUM responses with Memory_Unavailable Failure for Dialed Only number.	SUM
PES_ENUM_RSP_DIALED_ONLY_NO_NAME	COUNTER	False	Number of ENUM responses with Name_Does_Not_Exist Failure for Dialed Only number.	SUM

PSXPesFailureStats

Column Name	Column Type	Index	Description
QUERY_ERROR	COUNTER	No	The number of requests that encountered an SQL Query Error.
INTERNAL_ERROR	COUNTER	No	The number of requests that encountered an Internal Error.
EXTERNAL_ERROR	COUNTER	No	The number of requests that encountered an External Error.

PSXPesLcrStats

Column Name	Column Type	Index	Description
CALL_TYPE_INTRA_LATA	COUNTER	No	A count of how many LCR calls are identified as intra lata call type.
CALL_TYPE_INTER_LATA	COUNTER	No	A count of how many LCR calls are identified as inter lata call type.
CALL_TYPE_UNKNOWN	COUNTER	No	Number of A count of how many LCR calls are identified as unknown call type.
TOTAL_CALLS	COUNTER	No	The total number of LCR calls processed by the PSX.

PSXPesPerServiceCountersStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
PES_PERSERVICETYPE	STRING	True	Service Type.	False	N/A	Yes
PES_PERSERVICENAME	STRING	True	Service Name.	False	N/A	Yes

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
PES_REQSENT	COUNTER	False	Tracks the number of requests sent by the pes process counted for each Service.	True	SUM	Yes
PES_RESRECV	COUNTER	False	Tracks the number of responses received by the pes process counted for each Service.	True	SUM	Yes
PES_TIMEOUTS	COUNTER	False	Tracks the number of timeouts reached by the pes process counted for each Service.	True	SUM	Yes
PES_MISSINGPARAM	COUNTER	False	Tracks the number of Missing Request parameters by the pes process counted for each Service.	True	SUM	Yes
PES_PERSERVICECVT	COUNTER	False	Tracks number of times Call Validation and treatment executed.	True	SUM	Yes
PES_PERSERVICECVTESCAPED	COUNTER	False	Tracks number of times Call Validation and treatment escaped.	True	SUM	Yes
PES_PERSERVICEMISSINGPARAM	COUNTER	False	Tracks number of times Call Validation and treatment escaped.	True	SUM	Yes
PES_PERSERVICEMISSINGBODY NOTE: Available only for PSX 15.1.2	COUNTER	False	Tracks the number of all optional response parameters missing which have been received by the pes process counted for each service.	-	SUM	-

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
PES_PERSER VICEFAILURE4 XX NOTE: Available only for PSX 15.1.2	COUNTER	False	Tracks the number of failure due to 4XX error code which have been received by the pes process counted for each service.	-	SUM	-
PES_PERSER VICEFAILURE5 XX NOTE: Available only for PSX 15.1.2	COUNTER	False	Tracks the number of failure due to 5XX error code which have been received by the pes process counted for each service.	-	SUM	-
PES_PERSER VICEFAILURE6 XX NOTE: Available only for PSX 15.1.2	COUNTER	False	Tracks the number of failure due to 6XX error code which have been received by the pes process counted for each service.	-	SUM	-
PES_PERSER VICEFAILURE OTHER NOTE: Available only for PSX 15.1.2	COUNTER	False	Tracks the number of failure due to other error code which have been received by the pes process counted for each service.	-	SUM	-

PSXPesStiRcdCountersStats

Column Name	Column Type	Index	Description	Aggregation Type
STI_RCD_SIGN_REQ_ SUCCESS NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of embedded RCD in shaken and RCD only Signing Successful Request.	SUM
STI_RCD_SIGN_REQ_ FAILURE NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of embedded RCD in shaken and RCD only Signing Failure Request.	SUM

Column Name	Column Type	Index	Description	Aggregation Type
STI_RCD_SIGN_RES_SUCCESS NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of embedded RCD in shaken and RCD only Signing Successful Response.	SUM
STI_RCD_SIGN_RES_FAILURE NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of embedded RCD in shaken and RCD only Signing Failure Response.	SUM
CPS_STI_RCD_REQ_SUCCESS	INTEGER	-	Cps count of embedded RCD in shaken and RCD only Verification Successful Request.	SUM
CPS_STI_RCD_REQ_FAILURE	INTEGER	-	Cps count of embedded RCD in shaken and RCD only Verification Failure Request.	SUM
CPS_STI_RCD_RES_SUCCESS	INTEGER	-	Cps count of embedded RCD in shaken and RCD only Verification Successful Response.	SUM
CPS_STI_RCD_RES_FAILURE	INTEGER	-	Cps count of embedded RCD in shaken and RCD only Verification Failure Response.	SUM

PSXPesStiShakenRcdCountersStats

Column Name	Column Type	Index	Description	canAggregate
STI_SHAKEN_RCD_REQ_SUCCESS	COUNTER	false	Count of shaken, embedded RCD in shaken and RCD only Verification Successful Request.	true
STI_SHAKEN_RCD_REQ_FAILURE	COUNTER	false	Count of shaken, embedded RCD in shaken and RCD only Verification Failure Request.	true
STI_SHAKEN_RCD_RES_SUCCESS	COUNTER	false	Count of shaken, embedded RCD in shaken and RCD only Verification Successful Response.	true

Column Name	Column Type	Index	Description	canAggregate
STI_SHAKEN_RCD_RES_FAILURE	COUNTER	false	Count of shaken, embedded RCD in shaken and RCD only Verification Failure Response.	true
CPS_STI_SHAKEN_RCD_REQ_SUCCESS	INTEGER	-	Cps count of shaken, embedded RCD in shaken and RCD only Verification Successful Request.	true
CPS_STI_SHAKEN_RCD_REQ_FAILURE	INTEGER	-	Cps count of shaken, embedded RCD in shaken and RCD only Verification Failure Request.	true
CPS_STI_SHAKEN_RCD_RES_SUCCESS	INTEGER	-	Cps count of shaken, embedded RCD in shaken and RCD only Verification Successful Response.	true
CPS_STI_SHAKEN_RCD_RES_FAILURE	INTEGER	-	Cps count of shaken, embedded RCD in shaken and RCD only Verification Successful Response.	true
STI_SHAKEN_RCD_SIGN_REQ_SUCCESS NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of shaken, embedded RCD in shaken and RCD only Signing Successful Request.	SUM
STI_SHAKEN_RCD_SIGN_REQ_FAILURE NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of shaken, embedded RCD in shaken and RCD only Signing Failure Request.	SUM
STI_SHAKEN_RCD_SIGN_RES_SUCCESS NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of shaken, embedded RCD in shaken and RCD only Signing Successful Response.	SUM
STI_SHAKEN_RCD_SIGN_RES_FAILURE NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of shaken, embedded RCD in shaken and RCD only Signing Failure Response.	SUM

PSXPesStiShakenCountersStats

Column Name	Column Type	Index	Description	Aggregation Type
STI_SHAKEN_SIGN_REQ_SUCCESS NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of Shaken Signing Successful Request.	SUM
STI_SHAKEN_SIGN_REQ_FAILURE NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of Shaken Signing Failure Request.	SUM
STI_SHAKEN_SIGN_RESPONSE_SUCCESS NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of Shaken Signing Successful Response.	SUM
STI_SHAKEN_SIGN_RESPONSE_FAILURE NOTE: Available only for PSX 15.1.2	COUNTER	False	Count of Shaken Signing Failure Response.	SUM
CPS_STI_SHAKEN_REQUEST_SUCCESS	INTEGER	-	Cps calculation of count of Shaken Verification Successful Request.	
CPS_STI_SHAKEN_REQUEST_FAILURE	INTEGER	-	Cps count of Shaken Verification Failure Request.	
CPS_STI_SHAKEN_RESPONSE_SUCCESS	INTEGER	-	Cps count of Shaken Verification Successful Response	
CPS_STI_SHAKEN_RESPONSE_FAILURE	INTEGER	-	Cps count of Shaken Verification Failure Response	

PSXPesTranslationLookupCounters

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
PES_SERVICE_TYPE	STRING	True	Key1 Translation lookup service type.	False	N/A	Yes
PES_SERVICE_NAME	STRING	True	Key2 Translation lookup service name.	False	N/A	Yes
PES_LOOKUP_TOTAL	COUNTER	False	Total Translation lookup triggered per service.	True	SUM	Yes
PES_LOOKUP_SUCCESSES	COUNTER	False	Total number of Translation lookup per service that were successful.	True	SUM	Yes
PES_LOOKUP_FAILED	COUNTER	False	Total number of Translation lookup per service that failed.	True	SUM	Yes

PSXScpa

PSXScpaSipPerServerStats

Column Name	Column Type	Index	Description
SIP_IP_ADDR	STRING	Yes	The IP address of the SCP Server for which counters are collected.
SIP_IP_PORT	INTEGER	Yes	The Port of SCP Server for which counters are collected.
SIP_INVITE_SENT	COUNTER	No	Tracks the number of INVITE requests sent by SCPA process. Retransmissions of messages are not counted.
SIP_2XX_RCVD	COUNTER	No	Tracks the number of 2XX responses received by SCPA process for INVITE transaction. Retransmissions of messages are not counted.

Column Name	Column Type	Index	Description
SIP_3XX_RCVD	COUNTER	No	Tracks the number of 3XX responses received by SCPA process for INVITE transactions. Retransmissions of messages are not counted.
SIP_4XX_RCVD	COUNTER	No	Tracks the number of 4XX responses received by SCPA process for INVITE transactions. Retransmissions of messages are not counted
SIP_5XX_RCVD	COUNTER	No	Tracks the number of 5XX responses received by SCPA process for INVITE transactions. Retransmissions of messages are not counted.
SIP_6XX_RCVD	COUNTER	No	Tracks the number of 6XX responses received by SCPA process for INVITE transactions. Retransmissions of messages are not counted.
HPC_INVITE_SENT	INTEGER	Yes	Tracks the number of INVITE requests sent by the SCPA process for HPC Calls. Retransmissions of messages are not counted.
HPC_2XX_RCVD	INTEGER	Yes	Tracks the number of 2XX responses received by the SCPA proces for HPC Calls. Retransmissions of messages are not counted.
HPC_3XX_RCVD	INTEGER	Yes	Tracks the number of 3XX responses received by the SCPA process for INVITE transactions for HPC Calls. Retransmissions of messages are not counted.

Column Name	Column Type	Index	Description
HPC_4XX_RCVD	INTEGER	No	Tracks the number of 4XX responses received by the SCPA process for INVITE transactions for HPC Calls. Retransmissions of messages are not counted.
HPC_5XX_RCVD	INTEGER	No	Tracks the number of 5XX responses received by the SCPA process for INVITE transactions for HPC Calls. Retransmissions of messages are not counted.
HPC_6XX_RCVD	INTEGER	No	Tracks the number of 6XX responses received by the SCPA process for INVITE transactions for HPC Calls. Retransmissions of messages are not counted.

PSXScpaSipReqRespStats

Column Name	Column Type	Index	Description
SIP_INVITE_SENT	COUNTER	No	Tracks the number of INVITE requests sent by SCPA process. Retransmissions of messages are not counted.
SIP2_XX_RCVD	COUNTER	No	Tracks the number of 2XX responses received by SCPA process for INVITE transactions. Retransmissions of messages are not counted.
SIP3_XX_RCVD	COUNTER	No	Tracks the number of 3XX responses received by SCPA process for INVITE transactions. Retransmissions of messages are not counted.
SIP4_XX_RCVD	COUNTER	No	Tracks the number of 4XX responses received by SCPA process for INVITE transactions. Retransmissions of messages are not counted.

Column Name	Column Type	Index	Description
SIP5_XX_RCVD	COUNTER	No	Tracks the number of 5XX responses received by SCPA process for INVITE transactions. Retransmissions of messages are not counted.
SIP6_XX_RCVD	COUNTER	No	Tracks the number of 6XX responses received by SCPA process for INVITE transactions. Retransmissions of messages are not counted.
TIME_OUT_RCVD	COUNTER	No	Tracks the number of Transaction timeouts that happened for SIP-SCP calls.
HPC_INVITE	INTEGER	Yes	Tracks the number of HPC Invites sent out while encoding HPC Dscp Value.
HPC_SIP_2XX_RCVD	INTEGER	Yes	Tracks the number of 2XX responses received by the SCPA proces for HPC Calls. Retransmissions of messages are not counted.
HPC_SIP3_XX_RCVD	INTEGER	Yes	Tracks the number of 3XX responses received by the SCPA process for INVITE transactions for HPC Calls. Retransmissions of messages are not counted.
HPC_SIP4_XX_RCVD	INTEGER	No	Tracks the number of 4XX responses received by the SCPA process for INVITE transactions for HPC Calls. Retransmissions of messages are not counted.
HPC_SIP5_XX_RCVD	INTEGER	No	Tracks the number of 5XX responses received by the SCPA process for INVITE transactions for HPC Calls. Retransmissions of messages are not counted.
HPC_SIP6_XX_RCVD	INTEGER	No	Tracks the number of 6XX responses received by the SCPA process for INVITE transactions for HPC Calls. Retransmissions of messages are not counted.

Column Name	Column Type	Index	Description
HPC_TIME_OUT_RCVD	INTEGER	No	Tracks the number of Transaction timeouts for SIP-SCP HPC calls.

PSXScpaSipStats

Column Name	Column Type	Index	Description
ESRREQ_SENT	COUNTER	No	Keeps track of the number of Emergency Services Routing Requests (ESRReq) sent by the PSX.
TOTAL_ESRRSP_RCVD	COUNTER	No	Keeps track of the total number of Emergency Services Routing Responses (ESRRsp) received by the PSX.
SUCCESS_ESRRSP_RCVD	COUNTER	No	Keeps track of the number of successful Emergency Services Routing Responses (ESRRsp) received by the PSX.
FAILED_ESRRSP_RCVD	COUNTER	No	Keeps track of the number of failed Emergency Services Routing Responses (ESRRsp) received by the PSX.
ESRREQ_RETRY	COUNTER	No	Keeps track of the number of Emergency Services Routing Requests (ESRReq) retransmitted by the PSX. Every retry is to a new VPC.

PSXScpaSuaAssocStats

The PSXScpaSuaAssocStats table is deprecated in EMS 13.2.1 and later versions.

Column Name	Column Type	Index	Description
ASPACKACK_RX	COUNTER	No	Number of ASP Active Ack Association Msgs Rcvd

Column Name	Column Type	Index	Description
ASPACKACK_TX	COUNTER	No	Number of ASP Active Ack Association Msgs Sent
ASPACRX	COUNTER	No	Number of ASP Active Association Msgs Rcvd
ASPACTX	COUNTER	No	Number of ASP Active Association Msgs Sent
ASPDNACK_RX	COUNTER	No	Number of ASP Down Ack Association Msgs Rcvd
ASPDNACK_TX	COUNTER	No	Number of ASP Down Ack Association Msgs Sent
ASPDNRX	COUNTER	No	Number of ASP Down Association Msgs Rcvd
ASPDNTX	COUNTER	No	Number of ASP Down Association Msgs Sent
ASPIAACK_RX	COUNTER	No	Number of ASPIA Ack Association Msgs Rcvd
ASPIAACK_TX	COUNTER	No	Number of ASPIA Ack Association Msgs Sent
ASPIARX	COUNTER	No	Number of ASPIA Association Msgs Rcvd
ASPIATX	COUNTER	No	Number of ASPIA Association Msgs Sent
ASPMFAIL	COUNTER	No	Number of ASPM Association Failures
ASPUPACK_RX	COUNTER	No	Number of ASPUP Ack Association Msgs Rcvd
ASPUPACK_TX	COUNTER	No	Number of ASPUP Ack Association Msgs Sent
ASPUPRX	COUNTER	No	Number of ASPUP Association Msgs Rcvd

Column Name	Column Type	Index	Description
ASPUPTX	COUNTER	No	Number of ASPUP Association Msgs Sent
BEATAck_RX	COUNTER	No	Number of BEAT Ack Association Msgs Rcvd
BEATAck_TX	COUNTER	No	Number of BEAT Ack Association Msgs Sent
BEATRX	COUNTER	No	Number of BEAT Association Msgs Rcvd
BEATTX	COUNTER	No	Number of BEAT Association Msgs Sent
CLCOSIZE_RX	COUNTER64	No	Total Bytes of CL & CO Association Msgs Rcvd
CLCOSIZE_TX	COUNTER64	No	Total Bytes of CL & CO Association Msgs Sent
CLMSG_RX	COUNTER	No	Number of ConnectionLess Association Msgs Rcvd
CLMSG_TX	COUNTER	No	Number of ConnectionLess Association Msgs Sent
COMSG_RX	COUNTER	No	Number of ConnectionOriented Association Msgs Rcvd
COMSG_TX	COUNTER	No	Number of ConnectionOriented Association Msgs Sent
DAUDRX	COUNTER	No	Number of DAUD Association Msgs Rcvd
DAUDTX	COUNTER	No	Number of DAUD Association Msgs Sent
DAVARX	COUNTER	No	Number of DAVA Association Msgs Rcvd
DAVATX	COUNTER	No	Number of DAVA Association Msgs Sent

Column Name	Column Type	Index	Description
DE_REG_REQ_RX	COUNTER	No	Number of Dereg Req Association Msgs Rcvd
DE_REG_REQ_TX	COUNTER	No	Number of Dereg Req Association Msgs Sent
DE_REG_RSP_RX	COUNTER	No	Number of Dereg Rsp Association Msgs Rcvd
DE_REG_RSP_TX	COUNTER	No	Number of Dereg Rsp Association Msgs Sent
DRSTRX	COUNTER	No	Number of DUPU Association Msgs Rcvd
DRSTTX	COUNTER	No	Number of DUPU Association Msgs Sent
DUNARX	COUNTER	No	Number of DUNA Association Msgs Rcvd
DUNATX	COUNTER	No	Number of DUNA Association Msgs Sent
DUPURX	COUNTER	No	Number of DUPU Association Msgs Rcvd
DUPUTX	COUNTER	No	Number of DUPU Association Msgs Sent
ERR_RX	COUNTER	No	Number of Error Association Msgs Rcvd
ERR_TX	COUNTER	No	Number of Error Association Msgs Sent
LOCAL_IP	IPADDRESS	Yes	Local Host's IP address
LOCAL_PORT	INTEGER	Yes	Local Host's Port Number
NOTIFY_RX	COUNTER	No	Number of Association Notifications Rcvd

Column Name	Column Type	Index	Description
NOTIFY_TX	COUNTER	No	Number of Association Notifications Sent
PEER_IP	IPADDRESS	Yes	Remote Peer's IP address
PEER_PORT	INTEGER	Yes	Remote Peer's Port Number
REG_REQ_RX	COUNTER	No	Number of REG Req Association Msgs Rcvd
REG_REQ_TX	COUNTER	No	Number of REG Req Association Msgs Sent
REG_RSP_RX	COUNTER	No	Number of REG Rsp Association Msgs Rcvd
REG_RSP_TX	COUNTER	No	Number of REG Rsp Association Msgs Sent
SCONRX	COUNTER	No	Number of SCON Association Msgs Rcvd
SCONTX	COUNTER	No	Number of SCON Association Msgs Sent
SCTPTRANS_TIMEOUT	COUNTER	No	Number of SCTP Association Transmission Timeouts

PSXScpaSuaExtAssocStats

Column Name	Column Type	Index	Description	canAggregate
LOCAL_IP_TYPE	INTEGER	Yes	The IP address type of the ENUM localhost associated with the counter.	false
LOCAL_IP	STRING	Yes	The IP address of the localhost.	false
LOCAL_PORT	INTEGER	Yes	The port number of the localhost.	false

PEER_IP_TYPE	INTEGER	Yes	The IP address type of the ENUM Remote Peer associated with the counter.	false
PEER_IP	STRING	Yes	The IP address of the remote peer.	false
PEER_PORT	INTEGER	Yes	The port number of the remote peer.	false
CLMSG_TX	COUNTER	No	The count of connectionless association messages sent.	true
CLMSG_RX	COUNTER	No	The count of connectionless association messages received.	true
COMSG_TX	COUNTER	No	The count of connection-oriented association messages sent.	true
COMSG_RX	COUNTER	No	The count of connection-oriented association messages received.	true
CLCOSIZE_TX	COUNTER64	No	Total Bytes of connectionless and connection-oriented association messages sent.	true
CLCOSIZE_RX	COUNTER64	No	Total Bytes of connectionless and connection-oriented association messages received.	true
ERR_TX	COUNTER	No	The count of error association messages sent.	true
ERR_RX	COUNTER	No	The count of error association messages received.	true
NOTIFY_TX	COUNTER	No	The count of association notifications sent.	true
NOTIFY_RX	COUNTER	No	The count of association notifications received.	true

DUNATX	COUNTER	No	The count of DUNA association messages sent.	true
DUNARX	COUNTER	No	The count of DUNA association messages received.	true
DAVATX	COUNTER	No	The count of DAVA association messages sent.	true
DAVARX	COUNTER	No	The count of DAVA association messages received.	true
DAUDTX	COUNTER	No	The count of DAUD association messages sent.	true
DAUDRX	COUNTER	No	The count of DAUD association messages received.	true
SCONTX	COUNTER	No	The count of SCON association messages sent.	true
SCONRX	COUNTER	No	The count of SCON association messages received.	true
DUPUTX	COUNTER	No	The count of DUPU association messages sent.	true
DUPURX	COUNTER	No	The count of DUPU association messages received.	true
DRSTTX	COUNTER	No	The count of DUPU association messages sent.	true
DRSTRX	COUNTER	No	The count of DUPU association messages received.	true
ASPUPTX	COUNTER	No	The count of A USP association messages sent.	true
ASPUPRX	COUNTER	No	The count of A USP association messages received.	true
ASPUPACK_TX	COUNTER	No	The count of ASPUP acknowledgment association messages sent.	true

ASPUPACK_RX	COUNTER	No	The count of ASPUP acknowledgment association messages received.	true
ASPDNTX	COUNTER	No	The count of ASP DOWN association messages sent.	true
ASPDNRX	COUNTER	No	The count of ASP DOWN association messages received.	true
ASPDNACK_TX	COUNTER	No	The count of ASP DOWN acknowledgment association messages sent.	true
ASPDNACK_RX	COUNTER	No	The count of ASP DOWN acknowledgment association messages received.	true
BEATTX	COUNTER	No	The count of BEAT association messages sent.	true
BEATRX	COUNTER	No	The count of BEAT association messages received.	true
BEATAACK_TX	COUNTER	No	The count of BEAT acknowledgment association messages sent.	true
BEATAACK_RX	COUNTER	No	The count of BEAT acknowledgment association messages received.	true
ASPACTX	COUNTER	No	The count of ASP Active association messages sent.	true
ASPACRX	COUNTER	No	The count of ASP active association messages received.	true
ASPACKACK_TX	COUNTER	No	The count of ASP Active acknowledgment association messages sent.	true

ASPACKACK_RX	COUNTER	No	The count of ASP Active acknowledgment association messages received.	true
ASPIATX	COUNTER	No	The count of ASPIA association messages sent.	true
ASPIARX	COUNTER	No	The count of ASPIA association messages received.	true
ASPIAACK_TX	COUNTER	No	The count of ASPIA acknowledgment association messages sent.	true
ASPIAACK_RX	COUNTER	No	The count of ASPIA acknowledgment association messages received.	true
REG_REQ_TX	COUNTER	No	The count of REG Req association messages sent.	true
REG_REQ_RX	COUNTER	No	The count of REG Req association messages received.	true
REG_RSP_TX	COUNTER	No	The count of REG Rsp association messages sent.	true
REG_RSP_RX	COUNTER	No	The count of REG Rsp association messages received.	true
DE_REG_REQ_TX	COUNTER	No	The count of Dereg Req association messages sent.	true
DE_REG_REQ_RX	COUNTER	No	The count of Dereg Req association messages received.	true
DE_REG_RSP_TX	COUNTER	No	The count of Dereg Rsp association messages sent.	true

DE_REG_RSP_RX	COUNTER	No	The count of Dereg Rsp association messages received.	true
SCTPTRANS_TIME OUT	COUNTER	No	The count of SCTP association transmission timeouts.	true
ASPMFAIL	COUNTER	No	The count of ASPM association failures.	true

PSXScpaSuaProtocolStats

Column Name	Column Type	Index	Description
SCCPMGMT_MSG_TX	COUNTER	No	Total Number of SCCP Management messages sent.
SCCPMGMT_MSG_RX	COUNTER	No	Total Number of SCCP Management messages received.
CLMSG_TX	COUNTER	No	Total Number of ConnectionLess messages sent.
CLMSG_RX	COUNTER	No	Total Number of ConnectionLess messages received.
COMSG_TX	COUNTER	No	Total Number of ConnectionOriented messages sent.
COMSG_RX	COUNTER	No	Total Number of ConnectionOriented messages received.
CLCOSIZE_TX	COUNTER64	No	Total Bytes of Connection Less & Oriented messages Sent
CLCOSIZE_RX	COUNTER64	No	Total Bytes of Connection Less & Oriented messages received.
LOCAL_SSNMSG_RX	COUNTER	No	Total Number of messages received for Local SSN
GTTMSG	COUNTER	No	Total Number of messages requiring GTT

PSXScpaSuaRoutingStats

Column Name	Column Type	Index	Description
GTT_FAILS	COUNTER	No	Total Number of GTT Routing Failures.
SS_FAILS	COUNTER	No	Total Number of SubSystem Routing Failures.
NETWORK_FAILS	COUNTER	No	Total Number of Network Routing Failures.
NETWORK_CONGESTION	COUNTER	No	Total Number of Network Routing Congestions.
UNEQUIPPED_ERR	COUNTER	No	Total Number of Unequipped Users Routing Errors.
PC_NOT_CONFIG_ERR	COUNTER	No	Total Number of PC Not Configured Routing Errors.

PSXScpaSuaSSNStats

Column Name	Column Type	Index	Description
ID	INTEGER	Yes	Subsystem Number.
CLDTMSG_TX	COUNTER	No	Total Number of ConnectionLess messages Sent.
CLDTMSG_RX	COUNTER	No	Total Number of ConnectionLess messages received.
CODTMSG_TX	COUNTER	No	Total Number of ConnectionOriented messages Sent.
CODTMSG_RX	COUNTER	No	Total Number of ConnectionOriented messages received.

PSXSipeDnsStats

Column Name	Column Type	Index	Description
KA_REQ_SENT	COUNTER	No	The total number of KeepAlive requests sent by SIPE.
KA_RESP_RECEIVED	COUNTER	No	The total number of KeepAlive responses received by SIPE.
DNSCANCELED_REQUESTS	COUNTER	No	The total number of DNS requests canceled by SIPE.
LONG_TERM_AVG_TRANSACTION_TIME	GAUGE	No	The long term average of transaction time.
SHORT_TERM_AVG_TRANSACTION_TIME	GAUGE	No	The short term average of transaction time.
A_RES_REC_REQUESTS_SENT	COUNTER	No	The number of DNS A Resource Record requests sent by SIPE.
A_RES_REC_RESPONSES_RECEIVED	COUNTER	No	The number of DNS A Resource Record responses received by SIPE.
A_RES_REC_CANCELED_REQUESTS	COUNTER	No	The number of DNS A Resource Record requests canceled by SIPE.
A_RES_REC_RSP_SUCCESS	COUNTER	No	The number of Successful DNS A Resource Record Responses.
A_RES_REC_RSP_HOST_NOT_FOUND	COUNTER	No	The number of DNS A Resource Record Responses with Host_Not_Found Failure.
A_RES_REC_RSP_TRY_AGAIN	COUNTER	No	The number of DNS A Resource Record Responses with Temporary_Server_Error_Try_Again Failure.
A_RES_REC_RSP_NO_RECOVERY	COUNTER	No	The number of DNS A Resource Record Responses with Non_Recoverable_Name_Server_Error Failure.

Column Name	Column Type	Index	Description
A_RES_REC_RSP_NO_DATA	COUNTER	No	The number of DNS A Resource Record Responses with Valid_Name_But_No_Data_Record Failure.
NAPTR_RES_REC_REQUESTS_SENT	COUNTER	No	Number of DNS NAPTR Resource Record requests sent by SIPE.
NAPTR_RES_REC_RSP_RECEIVED	COUNTER	No	Number of DNS NAPTR Resource Record responses received by SIPE.
NAPTR_RES_REC_CANCEL_REQ	COUNTER	No	Number of DNS NAPTR Resource Record requests canceled by SIPE.
NAPTR_RES_REC_RSP_SUCCESS	COUNTER	No	Number of Successful DNS NAPTR Resource Record responses.
NAPTR_RES_REC_RSP_GENERAL_FAIL	COUNTER	No	Number of DNS NAPTR Resource Record responses with General Failure.
NAPTR_RES_REC_RSP_NOMEMORY	COUNTER	No	Number of DNS NAPTR Resource Record responses with Memory_Unavailable Failure.
NAPTR_RES_REC_RSP_INVALID_PARAM	COUNTER	No	Number of DNS NAPTR Resource Record responses with Invalid_Parameter Failure.
NAPTR_RES_REC_RSP_NO_NAME	COUNTER	No	Number of DNS NAPTR Resource Record responses with Name_Does_Not_Exist Failure.
NAPTR_RES_REC_RSP_NO_DATA	COUNTER	No	Number of DNS NAPTR Resource Record responses with Valid_Name_But_No_Data_Record Failure.
SRV_RES_REC_REQUESTS_SENT	COUNTER	No	Number of DNS SRV Resource Record requests sent by SIPE.
SRV_RES_REC_RSP_RECEIVED	COUNTER	No	Number of DNS NAPTR Resource Record responses received by SIPE.
SRV_RES_REC_CANCELLED_REQ	COUNTER	No	Number of SRV NAPTR Resource Record requests canceled by SIPE.

Column Name	Column Type	Index	Description
SRV_RES_REC_RSP_SUCCESS	COUNTER	No	Number of Successful SRV NAPTR Resource Record responses.
SRV_RES_REC_RSP_GEN_FAILURE	COUNTER	No	Number of DNS SRV Resource Record responses with General Failure.
RV_RES_REC_RSP_NOMEMORY	COUNTER	No	Number of DNS SRV Resource Record responses with Memory_Unavailable Failure.
SRV_RES_REC_RSP_INVALID_PARM	COUNTER	No	Number of DNS SRV Resource Record responses with Invalid_Parameter Failure.
SRV_RES_REC_RSP_NO_NAME	COUNTER	No	Number of DNS SRV Resource Record responses with Name_Does_Not_Exist Failure.
SRV_RES_REC_RSP_NO_DATA	COUNTER	No	Number of DNS SRV Resource Record responses with Valid_Name_But_No_Data_Record Failure.
AAAA_RES_REC_REQUESTS_SENT	COUNTER	No	Number of DNS AAAA Resource Record requests sent by SIPE
AAAA_RES_REC_RSP_RECEIVED	COUNTER	No	Number of DNS AAAA Resource Record responses received by SIPE.
AAAA_RES_REC_CANCELLED_REQ	COUNTER	No	Number of DNS AAAA Resource Record requests canceled by SIPE.
AAAA_RES_REC_RSP_SUCCESS	COUNTER	No	Number of Successful DNS AAAA Resource Record Responses.
AAAA_RES_REC_HOST_NOT_FOUND	COUNTER	No	Number of DNS AAAA Resource Record Responses with Host_Not_Found Failure.
AAAA_RES_REC_RSP_TRY	COUNTER	No	Number of DNS AAAA Resource Record Responses with Temporary_Server_Error_Try_Again Failure.

Column Name	Column Type	Index	Description
AAAA_RES_REC_RSP_NO RCOV	COUNTER	No	Number of DNS AAAA Resource Record Responses with Non_Recoverable_Name_Server_Error Failure.
AAAA_RES_REC_RSP_NO _DATA	COUNTER	No	Number of DNS AAAA Resource Record Responses with Valid_Name_But_No_Data_Record Failure.

PSXSipInternetworkingStats

Column Name	Column Type	Index	Description	canAggregate
SIPE_SIP1_18X_AC M_RECV	COUNTER	False	The number of SIP-I 18x with ISUP ACM received by SIPE.	False
SIPE_SIP1_18X_AC M_SENT	COUNTER	False	The number of SIP-I 18x with ISUP ACM sent by SIPE.	False
SIPE_SIP1_18X_CP G_RECV	COUNTER	False	The number of SIP-I 18x with ISUP CPG received by SIPE.	False
SIPE_SIP1_18X_CP G_SENT	COUNTER	False	The number of SIP-I 18x with ISUP CPG sent by SIPE.	False
SIPE_SIP1_200_AN M_RECV	COUNTER	False	The number of SIP-I 200 OK with ISUP ANM received by SIPE.	False
SIPE_SIP1_200_AN M_SENT	COUNTER	False	The number of SIP-I 200 OK with ISUP ANM sent by SIPE.	False
SIPE_SIP1_INVITE_ RECV	COUNTER	False	The number of SIP-I Invites with ISUP IAM received by SIPE.	False
SIPE_SIP1_INVITE_ SENT	COUNTER	False	The number of SIP-I Invites with ISUP IAM sent by SIPE.	False

PSXSoftswitch

PSXSoftSwitchHTTPClientPeakCPSUsageCountersStats

Column Name	Column Type	Index	Description	Aggregation Type
HTTP_PEAK_CPS_SIGN_QUERY_SENT	GAUGE	False	Tracks the peak CPS usages of signing queries sent.	Mean
HTTP_PEAK_CPS_SIGN_QUERY_RETRY	GAUGE	False	Tracks the peak CPS usages of signing queries retried.	Mean
HTTP_PEAK_CPS_VER_QUERY_SENT	GAUGE	False	Tracks the peak CPS usages of verification queries sent.	Mean
HTTP_PEAK_CPS_VER_QUERY_RETRY	GAUGE	False	Tracks the peak CPS usages of verification queries retried.	Mean

PSXSoftSwitchHttpRestUsagePerServiceCountersStats

Column Name	Column Type	Index	Description	Aggregation Type
REST_SERVICE_TYPE	STRING	True	Rest Service Type.	NA
REST_SERVICE_NAME	STRING	True	Rest Service Name.	NA

Column Name	Column Type	Index	Description	Aggregation Type
REST_USAGE_REQ_SENT	COUNTER64	False	This counter tracks the number of requests sent by the HTTP process towards REST server for each service.	SUM
REST_USGAE_PEAK_CPS	GAUGE	False	Peak CPS usage for each REST service.	Mean
CPS_REST_USAGE_REQ_SENT	GAUGE	False	Avg CPS of REST_USAGE_REQ_SENT.	Mean

PSXSoftSwitchPesCallStats

Column Name	Column Type	Index	Description
CCUSED	COUNTER	Yes	Number of call contexts that are currently in use.
CALLS_DROPPED	COUNTER	No	Number of calls that are dropped due to a lack of the call context available.

PSXSoftSwitchPesInapStats

Column Name	Column Type	Index	Description
IDP_SENT	COUNTER	No	The number of INAP Initial DP messages sent by the PSX.
IDP_FAILED	COUNTER	No	The number of INAP Initial DP messages that failed.
REQ_TIMEOUT	COUNTER	No	The number of INAP TSSF timeouts for request messages sent by the PSX.
ERROR_RCVD	COUNTER	No	The number of INAP User Error or Reject message received by the PSX.
ERROR_DETECTED	COUNTER	No	The number of INAP User Error or Reject messages sent by the PSX.

PSXSoftSwitchPesLicenseCountersStats

Column Name	Column Type	Index	Description	Aggregation Type
POL_TRANS_REQ_COUNTER	COUNTER	False	Counts the number of POL-TRANS-P(Local DB) License used.	SUM
PEAK_CPS_POL_TRANS_REQ	GAUGE	False	Peak CPS Usage of POL-TRANS-P(Local DB) License.	Mean
CVT_USAGE_TRIGGER	COUNTER 64	False	Counts the number of times CVT is triggered.	SUM
CVT_USAGE_PEAK_CPS	GAUGE	False	Peak CPS Usage of CVT.	Mean
CPS_CVT_USAGE_TRIGGER	INTEGER	-	Average CPS of CVT_USAGE_TRIGGER.	Mean

PSXSoftSwitchPesRcdCpsCounters

Column Name	Column Type	Index	Description	Aggregation Type
SHAKEN_RCD_SIGN_PEAK_CPS_COUNTER	GAUGE	False	Peak CPS Usage of SHAKEN RCD Signing Request.	Mean
RCD_SIGN_PEAK_CPS_COUNTER	GAUGE	False	Peak CPS Usage of RCD Signing Request.	Mean
SHAKEN_RCD_VERIFY_PEAK_CPS_COUNTER	GAUGE	False	Peak CPS Usage of SHAKEN RCD Verification Request.	Mean
RCD_VERIFY_PEAK_CPS_COUNTER	GAUGE	False	Peak CPS Usage of RCD Verification Request	Mean

PSXSoftSwitchScpaltuStats

Column Name	Column Type	Index	Description
QUERY_SENT	COUNTER	No	Tracks the number of ITU TCAP queries sent by the PSX.

Column Name	Column Type	Index	Description
QUERY_RCVD	COUNTER	No	Tracks the number of ITU TCAP queries received by the PSX.
TIMEOUT	COUNTER	No	Tracks the number of ITU TCAP queries which have timed out.
ERROR	COUNTER	No	Tracks the number of ITU TCAP error messages received by the PSX.
PURGED	COUNTER	No	Tracks the number of ITU TCAP queries purged by the PSX.
RSP_SENT	COUNTER	No	Tracks the number of ITU TCAP responses sent by the PSX.
RSP_RCVD	COUNTER	No	Tracks the number of ITU TCAP responses received by the PSX.
OPEN_TRANS	COUNTER	No	Tracks the number of ITU TCAP transactions which are still open pending for response.
DIALOG_ID_POOL_SIZE	COUNTER	No	Tracks the number of ITU TCAP dialog ids allocated by the PSX/SGX.
ABORT_RCVD	COUNTER	No	Tracks the number of ITU TCAP abort messages received by the PSX.
ABORT_SENT	COUNTER	No	Tracks the number of ITU TCAP abort messages sent by the PSX.
CONTINUE_RCVD	COUNTER	No	Tracks the number of ITU TCAP continue messages received by the PSX.
CONTINUE_SENT	COUNTER	No	Tracks the number of ITU TCAP continue messages sent by the PSX.
INVOKE_RCVD	COUNTER	No	Tracks the number of ITU TCAP Invoke components received by the PSX.
INVOKE_SENT	COUNTER	No	Tracks the number of ITU TCAP Invoke components sent by the PSX.

PSXSoftSwitchDIMAStats

Column Name	Column Type	Index	Description
STD_DIAMETER_MESG_SENT	COUNTER	No	Number of messages sent to Standard Diameter Peers.
STD_DIAMETER_MESG_RCVD	COUNTER	No	Number of messages received from Standard Diameter Peers.
MESG_SENT_TO_PES	COUNTER	No	Number of messages sent to PES.
MESG_RCVD_FROM_PES	COUNTER	No	Number of messages received from PES.
MESG_SENT_TO_SCPA	COUNTER	No	Number of messages sent to SCPA.
MESG_RCVD_FROM_SCPA	COUNTER	No	Number of messages received from SCPA.

PSXSoftSwitchDrmReqCountersStats

Column Name	Column Type	Index	Description	Aggregation Formula	Present in Reports
TOTAL_TDR_GEN	COUNTER	No	Total number of TDR generated.	SUM	No
TOTAL_PES_TDR_GEN	COUNTER	No	Total number of pes TDR generated.	SUM	No
TOTAL_SIPE_TDR_GEN	COUNTER	No	Total number of sipe TDR generated.	SUM	No
TDR_GEN_PS	COUNTER	No	Number of TDR generated per second.	SUM	No
TOTAL_TDR_GEN_PS	COUNTER	No	Number of PES TDR generated per second.	SUM	No
SIPE_TDR_GEN_PS	COUNTER	No	Number of SIPE TDR generated per second.	SUM	No

PSXSoftSwitchPesDnsEnumStats

Column Name	Column Type	Index	Description
DNSREQUESTS_SENT	COUNTER	No	Total number of DNS requests sent by the PSX
DNSRESPONSES_RECEIVED	COUNTER	No	Total number of DNS responses received by the PSX
ENUMREQUESTS_SENT	COUNTER	No	Total number of ENUM requests sent by the PSX
ENUMRESPONSES_RECEIVED	COUNTER	No	Total number of ENUM responses received by the PSX
KAREQUESTS_SENT	COUNTER	No	Total number of KeepAlive requests sent by the PSX
KARESPONSES_RECEIVED	COUNTER	No	Total number of KeepAlive responses received by the PSX
ENUMRESPONSE_SUCCESS	COUNTER	No	Total number of Successful ENUM responses
ENUMRESPONSE_GENERAL_FAILURE	COUNTER	No	Total number of ENUM responses with General Failure
ENUMRESPONSE_NO_MEMORY	COUNTER	No	Total number of ENUM responses with Memory_Unavailable Failure
ENUMRESPONSE_INVALID_PARAMETER	COUNTER	No	Total number of ENUM responses with Invalid_Parameter Failure
ENUMRESPONSE_NO_NAME	COUNTER	No	Total number of ENUM responses with Name_Does_Not_Exist Failure
ENUMRESPONSE_NO_DATA	COUNTER	No	Total number of ENUM responses with Valid_Name_But_No_Data_Record Failure
DNS_CANCELED_REQUESTS	COUNTER	No	Total number of DNS requests canceled by the PSX
ENUM_CANCELED_REQUESTS	COUNTER	No	Total number of ENUM requests canceled by the PSX

Column Name	Column Type	Index	Description
LONG_TERM_AVG_TRANSACTION_TIME	GAUGE	No	Long term average of transaction time
SHORT_TERM_AVG_TRANSACTION_TIME	GAUGE	No	Short term average of transaction time
NAPTR_REQUESTS_SENT	COUNTER	No	Number of DNS NAPTR Resource Record requests sent by the PSX
NAPTR_RESPONSES_RECEIVED	COUNTER	No	Number of DNS NAPTR Resource Record responses received by the PSX
NAPTR_CANCELED_REQUESTS	COUNTER	No	Number of DNS NAPTR Resource Record requests canceled by the PSX
NAPTR_RSP_SUCCESS	COUNTER	No	Number of Successful DNS NAPTR Resource Record responses
NAPTR_RSP_GENERAL_FAILURE	COUNTER	No	Number of DNS NAPTR Resource Record responses with General Failure
NAPTR_RSP_NO_MEMORY	COUNTER	No	Number of DNS NAPTR Resource Record responses with Memory_Unavailable Failure
NAPTR_RSP_INVALID_PARAM	COUNTER	No	Number of DNS NAPTR Resource Record responses with Invalid_Parameter Failure
NAPTR_RSP_NO_NAME	COUNTER	No	Number of DNS NAPTR Resource Record responses with Name_Does_Not_Exist Failure
NAPTR_RSP_NO_DATA	COUNTER	No	Number of DNS NAPTR Resource Record responses with Valid_Name_But_No_Data_Record Failure.
SRV_REQUESTS_SENT	COUNTER	No	Number of DNS SRV Resource Record requests sent by the PSX
SRV_RESPONSES_RECEIVED	COUNTER	No	Number of DNS SRV Resource Record responses received by the PSX
SRV_CANCELED_REQUESTS	COUNTER	No	Number of DNS SRV Resource Record requests canceled by the PSX
SRV_RSP_SUCCESS	COUNTER	No	Number of Successful DNS SRV Resource Record responses

Column Name	Column Type	Index	Description
SRV_RSP_GENERAL_FAILURE	COUNTER	No	Number of DNS SRV Resource Record responses with General Failure
SRV_RSP_NO_MEMORY	COUNTER	No	Number of DNS SRV Resource Record responses with Memory_Unavailable Failure
SRV_RSP_INVALID_PARAMETER	COUNTER	No	Number of DNS SRV Resource Record responses with Invalid_Parameter Failure
SRV_RSP_NO_NAME	COUNTER	No	Number of DNS SRV Resource Record responses with Name_Does_Not_Exist Failure
SRV_RSP_NO_DATA	COUNTER	No	Number of DNS SRV Resource Record responses with Valid_Name_But_No_Data_Record Failure
A_REQUESTS_SENT	COUNTER	No	Number of DNS A Resource Record requests sent by the PSX
A_RESPONSES_RECEIVED	COUNTER	No	Number of DNS A Resource Record responses received by the PSX
A_CANCELED_REQUESTS	COUNTER	No	Number of DNS A Resource Record requests canceled by the PSX
A_RSP_SUCCESS	COUNTER	No	Number of Successful DNS A Resource Record responses
A_RSP_HOST_NOT_FOUND	COUNTER	No	Number of DNS A Resource Record Responses with Host_Not_Found Failure
A_RSP_TRY_AGAIN	COUNTER	No	Number of DNS A Resource Record Responses with Temporary_Server_Error_Try_Again Failure
A_RSP_NO_RECOVERY	COUNTER	No	Number of DNS A Resource Record Responses with Non_Recoverable_Name_Server_Error Failure
A_RSP_NO_DATA	COUNTER	No	Number of DNS A Resource Record Responses with Valid_Name_But_No_Data_Record Failure
ENUMLNPREQUESTS_SENT	COUNTER	No	Total number of ENUM requests sent for LNP by the PSX
ENUMCNAMREQUESTS_SENT	COUNTER	No	Total number of ENUM requests sent for CNAM by the PSX

Column Name	Column Type	Index	Description
AAAA_RECORD_REQUESTS_SENT	COUNTER	No	Number of DNS AAAA Resource Record requests sent by the PSX
AAAA_RECORD_RESPONSES_RECEIVED	COUNTER	No	Number of DNS AAAA Resource Record responses received by the PSX
AAAA_RECORD_CANCELED_REQUESTS	COUNTER	No	Number of DNS AAAA Resource Record requests canceled by the PSX
AAAA_RECORD_RSP_SUCCESS	COUNTER	No	Number of Successful DNS AAAA Resource Record Responses
AAAA_RECORD_RSP_HOST_NOT_FOUND	COUNTER	No	Number of DNS AAAA Resource Record Responses with Host_Not_Found Failure
AAAA_RECORD_RSP_TRY_AGAIN	COUNTER	No	Number of DNS AAAA Resource Record Responses with Temporary_Server_Error_Try_Again Failure
AAAA_RECORD_RSP_NO_RECOVERY	COUNTER	No	Number of DNS AAAA Resource Record Responses with Non_Recoverable_Name_Server_Error Failure
AAAA_RECORD_RSP_NO_DATA	COUNTER	No	Number of DNS AAAA Resource Record Responses with Valid_Name_But_No_Data_Record Failure

PSXSsPesInboundEnumStats

Column Name	Column Type	Index	Description
TOTAL_REQUESTS_RECEIVED	COUNTER	No	The total number of Inbound ENUM requests received by the PSX.
TOTAL_RESPONSES_SENT	COUNTER	No	The total number of ENUM responses sent by the PSX.
TOTAL_SUCCESS_RESPONSES_SENT	COUNTER	No	The total number of Successful ENUM responses sent by the PSX.
SERV_FAILURE_RESPONSE_SENT	COUNTER	No	The total number of Server Failure ENUM responses sent by the PSX.

Column Name	Column Type	Index	Description
NAME_ERROR_RESPONSE_SENT	COUNTER	No	The total number of Name Error ENUM responses sent by the PSX.
TRANSPARENT_SUCCESS_RESPONSE_SENT	COUNTER	No	Total number of successful ENUM responses sent transparently.

PsxStirShakenStats

Column Name	Column Type	Index	Description	canAggregate
RED_SIGNED_CALLS	COUNTER	false	Tracks the number of signed calls in Redirector mode.	false
RED_VER_CALLS	COUNTER	false	Tracks the number of verified calls in Redirector mode.	false
RED_TAGD_CALLS	COUNTER	false	Tracks the number of tagged calls in Redirector mode.	false
PROXY_SIGNED_CALLS	COUNTER	false	Tracks the number of signed calls in Proxy mode.	false
PROXY_VER_CALLS	COUNTER	false	Tracks the number of verified calls in Proxy mode.	false
PROXY_TAGD_CALLS	COUNTER	false	Tracks the number of tagged calls in Proxy mode.	false

PSXTM

PSXTMCdDNDestAllowStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
ENTITY	STRING	Yes	Entity Id (national number) for called destination with traffic control
ENTITY2	STRING	Yes	Entity Id2 (country id) for called destination with traffic control
VALUE	COUNTER	No	Number of allowed calls to called destination with traffic control

PSXTMCdDNDestBlockStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
ENTITY	STRING	Yes	Entity Id (national number) for called destination with traffic control
ENTITY2	STRING	Yes	Entity Id2 (country id) for called destination with traffic control
VALUE	COUNTER	No	Number of blocked calls to called destination with traffic control

PSXTMContractorOrigAllowStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
ENTITY	STRING	Yes	Entity Id (national number) for contractor number based origination with traffic control
ENTITY2	STRING	Yes	Entity Id2 (country id) for contractor number based origination with traffic control
VALUE	COUNTER	No	Number of allowed calls from contractor number based origination with traffic control

PSXTMContractorOrigBlockStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
ENTITY	STRING	Yes	Entity Id (national number) for contractor number based origination with traffic control
ENTITY2	STRING	Yes	Entity Id2 (country id) for contractor number based origination with traffic control
VALUE	COUNTER	No	Number of blocked calls from contractor number based origination with traffic control

PSXTMCPEGroup

PSXTMCPEGroupPreProcessingAllowedStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
ENTITY	Entity	True	Entity Id (Generic Criteria Group Profile) for CPE Group at Pre-Processing with traffic control.	False	N/A	Yes
ENTITY2	Entity	True	Entity Id2 (Sonus_NULL) for CPE Group at Pre-Processing with traffic control.	False	N/A	Yes
VALUE	COUNTER	False	Number of allowed calls to CPE Group at Pre-Processing with traffic control.	True	SUM	Yes

PSXTMCPEGroupPreProcessingBlockedStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
ENTITY	Entity	True	Entity Id (Generic Criteria Group Profile) for CPE Group at Pre-Processing with traffic control.	False	N/A	Yes
ENTITY2	Entity	True	Entity Id2 (Sonus_NULL) for CPE Group at Pre-Processing with traffic control	False	N/A	Yes
VALUE	COUNTER	False	Number of blocked calls to CPE Group at Pre-Processing with traffic control.	True	SUM	Yes

PSXTMCPEGroupPreRoutingAllowedStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
ENTITY	Entity	True	Entity Id (Generic Criteria Group Profile) for CPE Group at Pre-Routing with traffic control.	False	N/A	Yes
ENTITY2	Entity	True	Entity Id2 (Sonus_NULL) for CPE Group at Pre-Routing with traffic control.	False	N/A	Yes
VALUE	COUNTER	False	Number of allowed calls to CPE Group at Pre-Routing with traffic control.	True	SUM	Yes

PSXTMCPEGroupPreRoutingBlockedStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
ENTITY	Entity	True	Entity Id (Generic Criteria Group Profile) for CPE Group at Pre-Routing with traffic control.	False	N/A	Yes
ENTITY2	Entity	True	Entity Id2 (Sonus_NULL) for CPE Group at Pre-Routing with traffic control	False	N/A	Yes
VALUE	COUNTER	False	Number of blocked calls to CPE Group at Pre-Routing with traffic control.	True	SUM	Yes

PSXTMCPEGroupPostRoutingAllowedStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
ENTITY	Entity	True	Entity Id (Generic Criteria Group Profile) for CPE Group at Post-Routing with traffic control.	False	N/A	Yes
ENTITY2	Entity	True	Entity Id2 (Sonus_NULL) for CPE Group at Post-Routing with traffic control.	False	N/A	Yes
VALUE	COUNTER	False	Number of allowed calls to CPE Group at Post-Routing with traffic control.	True	SUM	Yes

PSXTMCPEGroupPostRoutingBlockedStats

Column Name	Column Type	Index	Description	CanAggregate	Aggregation Formula	Present in Reports
ENTITY	Entity	True	Entity Id (Generic Criteria Group Profile) for CPE Group at Post-Routing with traffic control.	False	N/A	Yes
ENTITY2	Entity	True	Entity Id2 (Sonus_NULL) for CPE Group at Post-Routing with traffic control.	False	N/A	Yes
VALUE	COUNTER	False	Number of blocked calls to CPE Group at Post-Routing with traffic control.	True	SUM	Yes

PSXTMHpcExemptionStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
GSX_NAME	STRING	No	The name of the GSX to which the Traffic Management HPC Exemption counters apply
EXEMPTED_CALLS	COUNTER	No	The Traffic Management HPC Exemption counters per GSX count exempted calls that are traffic control exempted for any reason AND HPC call

PSXTriggeredService**PSXTriggeredServiceStats**

Column Name	Column Type	Index	Description	canAggregate
TRIGG_SERVICE_NAME	STRING	true	The name of the service that triggered the counters as the license is available.	false
TRIGG_SERVICE_COUNT	COUNTER64	false	The number of times service triggered.	true

PSXTriggeredServiceStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
TRIGG_SERVICE_NAME	STRING	true	The name of the service that triggered the counters as the license is available.	false	NA
TRIGG_SERVICE_COUNT	COUNTER64	false	The number of times service triggered.	true	SUM

PsxVerificationFailStats

Column Name	Column Type	Index	Description	canAggregate
VERIFICATION_FAILURE_E3	COUNTER	False	Keeps track of the number of E3 error received from verification server.	False
VERIFICATION_FAILURE_E4	COUNTER	False	Keeps track of the number of E4 error received from verification server.	False
VERIFICATION_FAILURE_E5	COUNTER	False	Keeps track of the number of E5 error received from verification server.	False
VERIFICATION_FAILURE_E6	COUNTER	False	Keeps track of the number of E6 error received from verification server.	False
VERIFICATION_FAILURE_E7	COUNTER	False	Keeps track of the number of E7 error received from verification server.	False
VERIFICATION_FAILURE_E8	COUNTER	False	Keeps track of the number of E8 error received from verification server.	False
VERIFICATION_FAILURE_E9	COUNTER	False	Keeps track of the number of E9 error received from verification server.	False
VERIFICATION_FAILURE_E10	COUNTER	False	Keeps track of the number of E10 error received from verification server.	False
VERIFICATION_FAILURE_E11	COUNTER	False	Keeps track of the number of E11 error received from verification server.	False
VERIFICATION_FAILURE_E12	COUNTER	False	Keeps track of the number of E12 error received from verification server.	False
VERIFICATION_FAILURE_E13	COUNTER	False	Keeps track of the number of E13 error received from verification server.	False
VERIFICATION_FAILURE_E14	COUNTER	False	Keeps track of the number of E14 error received from verification server.	False
VERIFICATION_FAILURE_E15	COUNTER	False	Keeps track of the number of E15 error received from verification server.	False

Column Name	Column Type	Index	Description	canAggregate
VERIFICATION_FAILURE_E16	COUNTER	False	Keeps track of the number of E16 error received from verification server.	False
VERIFICATION_FAILURE_E17	COUNTER	False	Keeps track of the number of E17 error received from verification server.	False
VERIFICATION_FAILURE_E18	COUNTER	False	Keeps track of the number of E18 error received from verification server.	False
VERIFICATION_FAILURE_E19	COUNTER	False	Keeps track of the number of E19 error received from verification server.	False
VERIFICATION_FAILURE_E20	COUNTER	False	Keeps track of the number of E20 error received from verification server.	False
VERIFICATION_FAILURE_E21	COUNTER	False	Keeps track of the number of E21 error received from verification server.	False
VERIFICATION_FAILURE_E22	COUNTER	False	Keeps track of the number of E22 error received from verification server.	False
VERIFICATION_FAILURE_E23	COUNTER	False	Keeps track of the number of E23 error received from verification server.	False
VERIFICATION_FAILURE_X1	COUNTER	False	Keeps track of the number of X1 error received from verification server.	False
VERIFICATION_FAILURE_X2	COUNTER	False	Keeps track of the number of X2 error received from verification server.	False
VERIFICATION_FAILURE_X3	COUNTER	False	Keeps track of the number of X3 error received from verification server.	False
VERIFICATION_FAILURE_X4	COUNTER	False	Keeps track of the number of X4 error received from verification server.	False
VERIFICATION_FAILURE400	COUNTER	False	Keeps track of the number of 400 error received from verification server.	False
VERIFICATION_FAILURE404	COUNTER	false	Tracks the number of 404 error received from verification server.	false
VERIFICATION_FAILURE405	COUNTER	true	Tracks the number of 405 error received from verification server.	false

Column Name	Column Type	Index	Description	canAggregate
VERIFICATION_FAILURE406	COUNTER	false	Tracks the number of 406 error received from verification server.	false
VERIFICATION_FAILURE411	COUNTER	false	Tracks the number of 411 error received from verification server.	false
VERIFICATION_FAILURE415	COUNTER	false	Tracks the number of 415 error received from verification server.	false
VERIFICATION_FAILURE500	COUNTER	False	Keeps track of the number of 500 error received from verification server.	False
VERIFICATION_FAILURE503	COUNTER	False	Keeps track of the number of 503 error received from verification server.	False
VERIFICATION_FAILURESVC4000	COUNTER	false	Tracks the number of service exception 4000 error received from verification server.	false
VERIFICATION_FAILURESVC4001	COUNTER	false	Tracks the number of service exception 4001 error received from the verification server.	false
VERIFICATION_FAILURESVC4002	COUNTER	false	Tracks the number of service exception 4002 error received from the verification server.	false
VERIFICATION_FAILURESVC4003	COUNTER	false	Tracks the number of service exception 4003 error received from the verification server.	false
VERIFICATION_FAILURESVC4004	COUNTER	false	Tracks the number of service exception 4004 error received from the verification server.	false
VERIFICATION_FAILURESVC4005	COUNTER	false	Tracks the number of service exception 4005 error received from the verification server.	false
VERIFICATION_FAILURESVC4006	COUNTER	false	Tracks the number of service exception 4006 error received from the verification server.	false
VERIFICATION_FAILURESVC4007	COUNTER	false	Tracks the number of service exception 4007 error received from the verification server.	false

Column Name	Column Type	Index	Description	canAggregate
VERIFICATION_FAILUREPOL4050	COUNTER	false	Tracks the number of service exception 4050 error received from the verification server.	false
VERIFICATION_FAILUREPOL5000	COUNTER	false	Tracks the number of service exception 5000 error received from the verification server.	false

ScpaStats

Column Name	Column Type	Index	Description
OPEN_CONVERSATIONS	COUNTER	No	Records the number of open conversation transactions at a given time.

ServiceUsageStats

Column Name	Column Type	Index	Description
DEFAULT_SVCS	COUNTER	No	Default Service: Tracks how many times default service is executed. The counter is incremented when no service is provisioned and the default service is executed.
SUBS_SCREENING	COUNTER	No	Subscriber Screening: Keeps track of how many times Subscriber Screening Service is executed. The counter is incremented when screening service provisioned for subscriber is executed.
SUBS_BLOCKING	COUNTER	No	Subscriber Blocking: Tracks how many times Subscriber Blocking Service is executed. The counter is incremented when blocking service provisioned for subscriber is executed.

Column Name	Column Type	Index	Description
NON_SUBS_SCREENING	COUNTER	No	Non Subscriber Screening: Tracks how many times Non Subscriber Screening Service is executed. This counter is incremented when the calling party is not present in the Subscriber database table and the nonsubscriber call is screened.
NON_SUBS_BLOCKING	COUNTER	No	Non Subscriber Blocking: Tracks how many times Subscriber Blocking Service is executed. This counter is incremented when the calling party is not present in the Subscriber database table and the nonsubscriber call is blocked.
SUBS_FORCED_ROUTING	COUNTER	No	Subscriber Forced Routing: Tracks how many times Subscriber Forced Routing Service is executed. The counter is incremented when forced routing service provisioned for subscriber is executed.
SUBS_HI_FRAUD_BLOCKING	COUNTER	No	Subscriber HiFraud Blocking: Tracks how many times Subscriber HiFraud Blocking Service is executed. The counter is incremented when HiFraud Blocking service provisioned for subscriber is executed.
SUBS_SAC_NON_SAC_ROUTES	COUNTER	No	Subscriber SAC/NonSAC Routes: Tracks how many times Subscriber SAC/NonSAC Routing Service is executed. The counter is incremented when SAC/NonSAC Routing service provisioned for subscriber is executed.
DEST_NUM_FORCED_ROUTING	COUNTER	No	Destination Number Forced Routing: Tracks how many times Destination Number Forced Routing Service is executed. The counter is incremented when Destination Number Forced Routing service provisioned for subscriber, Carrier, Trunk group or Gateway is executed.

Column Name	Column Type	Index	Description
CIC_PHONE_SCREENING	COUNTER	No	CIC Phone Screening: Tracks how many times incoming phone type calls are not allowed.
CIC_SCREENING	COUNTER	No	CIC Screening: Tracks how many times CIC Screening Service is executed. The counter is incremented when screening service provisioned for carrier is executed.
CIC_BLOCKING	COUNTER	No	CIC Blocking: Tracks how many times CIC Blocking Service is executed. The counter is incremented when blocking service provisioned for carrier is executed.
CIC_FORCED_ROUTING	COUNTER	No	CIC Forced Routing: Tracks how many times CIC Forced Routing Service is executed. The counter is incremented when Forced Routing service provisioned for carrier is executed.
CIC_HI_FRAUD_BLOCKING	COUNTER	No	CIC HiFraud Blocking: Tracks how many times CIC HiFraud Blocking Service is executed. The counter is incremented when HiFraud Blocking service provisioned for carrier is executed.
CIC_SAC_NON_SAC_ROUTES	COUNTER	No	CIC SAC/NonSAC Routes: Tracks how many times CIC SAC/NonSAC Routing Service is executed. The counter is incremented when SAC/NonSAC Routing service provisioned for carrier is executed.
TRUNKGROUP_SCREENING	COUNTER	No	Trunk group Screening: Tracks how many times Trunk group Screening Service is executed. The counter is incremented when screening service provisioned for trunk group is executed.

Column Name	Column Type	Index	Description
TRUNKGROUP_BLOCKING	COUNTER	No	Trunk group Blocking: Tracks how many times Trunk group Blocking Service is executed. The counter is incremented when blocking service provisioned for trunk group is executed.
TRUNKGROUP_FORCED_ROUTING	COUNTER	No	Trunk group Forced Routing: Tracks how many times Trunk group Forced Routing Service is executed. The counter is incremented when forced routing service provisioned for trunk group is executed.
TRUNKGROUP_HI_FRAUD_BLOCKING	COUNTER	No	Trunk group HiFraud Blocking: Tracks how many times Trunk group HiFraud Blocking Service is executed. The counter is incremented when HiFraud service provisioned for trunk group is executed.
TRUNKGROUP_SAC_NON_SAC_ROUTES	COUNTER	No	Trunk group SAC/NonSAC Routes: Tracks how many times Trunk group SAC/NonSAC Routing Service is executed. The counter is incremented when SAC/NonSAC Routing service provisioned for trunk group is executed.
CASUAL_CALL_UNALLOWED	COUNTER	No	Casual calls not allowed: Tracks how many times casual calls are not allowed through the network. The counter is incremented when the explicitly dialed carrier code incoming call type (for example, 1010321) is not allowed at one of the following levels of granularity: Infodigit, Carrier, Trunk group, Gateway, and SoftSwitch.
NON_SUBSCRIBER_CALLS_UNALLOWED	COUNTER	No	Non Subscriber calls not allowed: Tracks how many times non subscriber calls are not allowed through the network. This counter is incremented when a calling party is not present in the subscriber database and the casual routing is not allowed at Carrier, Trunk group, or Gateway level.

Column Name	Column Type	Index	Description
GATEWAY_SCREENING	COUNTER	No	Gateway Screening: Tracks how many times Gateway Screening Service is executed. The counter is incremented when screening service provisioned for gateway is executed.
GATEWAY_BLOCKING	COUNTER	No	Gateway Blocking: Tracks how many times Gateway Blocking Service is executed. The counter is incremented when blocking service provisioned for gateway is executed.
GATEWAY_FORCED_ROUTING	COUNTER	No	Gateway Forced Routing: Tracks how many times Gateway Forced Routing Service is executed. The counter is incremented when Forced Routing service provisioned for gateway is executed.
GATEWAY_HI_FRAUD_BLOCKING	COUNTER	No	Gateway HiFraud Blocking: Tracks how many times Gateway HiFraud Blocking Service is executed. The counter is incremented when HiFraud Blocking service provisioned for gateway is executed.
GATEWAY_SAC_NON_SAC_ROUTES	COUNTER	No	Gateway SAC/NonSAC Routes: Tracks how many times Gateway SAC/NonSAC Routing Service is executed. The counter is incremented when SAC/NonSAC Routing service provisioned for gateway is executed.
AUTH_CODE_SCREENING	COUNTER	No	Authcode Screening: Tracks how many times the Authcode Screening Service is executed. The counter is incremented when the screening service provisioned for Authcode is executed.

Column Name	Column Type	Index	Description
AUTH_CODE_BLOCKING	COUNTER	No	Authcode Blocking: Tracks how many times the Authcode Blocking service is executed. The counter is incremented when the blocking service provisioned for Authcode is executed.
AUTH_CODE_FORCED_ROUTING	COUNTER	No	Authcode Forced Routing: Keeps track of how many times the Authcode Forced Routing service is executed. The counter is incremented when the Forced Routing service provisioned for Authcode is executed.
UTHCODE_HI_FRAUD_BLOCKING	COUNTER	No	Authcode HiFraud Blocking: Keeps track of how many times the Authcode HiFraud Blocking service is executed. The counter is incremented when the HiFraud Blocking service provisioned for Authcode is executed.
AUTH_CODE_SAC_NON_SAC_ROUTES	COUNTER	No	Authcode SAC/NonSAC Routes: Keeps track of how many times the Authcode SAC/NonSAC Routing service is executed. The counter is incremented when the SAC/NonSAC Routing service provisioned for Authcode is executed.
INFO_DIGIT_SCREENING	COUNTER	No	Infodigit Screening: Keeps track of how many times the Infodigit Screening Service is executed. The counter is incremented when the screening service provisioned for Infodigit is executed.
INFO_DIGIT_BLOCKING	COUNTER	No	Infodigit Blocking: Keeps track of how many times the Infodigit Blocking service is executed. The counter is incremented when the blocking service provisioned for Infodigit is executed.
INFO_DIGIT_FORCED_ROUTING	COUNTER	No	Infodigit Forced Routing: Keeps track of how many times the Infodigit Forced Routing service is executed. The counter is incremented when the Forced Routing service provisioned for Infodigit is executed.

Column Name	Column Type	Index	Description
INFO_DIGIT_HI_FRAUD_BLOCKING	COUNTER	No	Infodigit HiFraud Blocking: Keeps track of how many times the Infodigit HiFraud Blocking service is executed. The counter is incremented when the HiFraud Blocking service provisioned for Infodigit is executed.
INFO_DIGIT_SAC_NON_SAC_ROUTES	COUNTER	No	Infodigit SAC/NonSAC Routes: Keeps track of how many times the Infodigit SAC/NonSAC Routing service is executed. The counter is incremented when the SAC/NonSAC Routing service provisioned for Infodigit is executed.
SOFTSWITCH_SCREENING	COUNTER	No	Softswitch Screening: Keeps track of how many times the SoftSwitch Screening Service is executed. The counter is incremented when the screening service provisioned for SoftSwitch is executed.
SOFTSWITCH_BLOCKING	COUNTER	No	Softswitch Blocking: Keeps track of how many times the SoftSwitch Blocking service is executed. The counter is incremented when the blocking service provisioned for SoftSwitch is executed.
SOFTSWITCH_FORCED_ROUTING	COUNTER	No	Softswitch Forced Routing: Keeps track of how many times the SoftSwitch Forced Routing service is executed. The counter is incremented when the Forced Routing service provisioned for SoftSwitch is executed.
SOFTSWITCH_HI_FRAUD_BLOCKING	COUNTER	No	Softswitch HiFraud Blocking: Keeps track of how many times the SoftSwitch HiFraud Blocking service is executed. The counter is incremented when the HiFraud Blocking service provisioned for SoftSwitch is executed.
SOFTSWITCH_SAC_NON_SAC_ROUTES	COUNTER	No	Softswitch SAC/NonSAC Routes: Keeps track of how many times the SoftSwitch SAC/NonSAC Routing service is executed. The counter is incremented when the SAC/NonSAC Routing service provisioned for SoftSwitch is executed.

SoftSwitchLwresd**SoftSwitchLwresdServerStats**

Column Name	Column Type	Index	Description	Aggregation Type
SERVER_IP_ADDRESSTYPE	INTEGER	True	The ENUM Server IP address Type that the Counters apply to.	NA
SERVER_IP_ADDRESS	STRING	True	The ENUM Server IP address that the Counters apply to.	NA
SERVER_PORT	INTEGER	True	The Port on which ENUM server is listening.	NA
SERVER_TRANSPORTTYPE	INTEGER	True	The transport used towards the ENUM server.	NA
NAPTR_REQUEST	COUNTER	False	Keeps track of the number of NAPTR requests sent to the ENUM server.	SUM
NAPTR_RESPONSE	COUNTER	False	Keeps track of the number of NAPTR responses received from the ENUM server.	SUM
NAPTR_NO_ANS_RESPONSE	COUNTER	False	Keeps track of the number of NAPTR no answer responses.	SUM
NAPTR_REQUEST_TIMEOUT	COUNTER	False	Keeps track of the number of NAPTR request timeouts.	SUM
NAPTR_DEST_UNREACHABLE	COUNTER	False	Keeps track of the number of NAPTR destination unreachable counts.	SUM
SRV_REQUEST	COUNTER	False	Keeps track of the number of SRV requests sent to the DNS server.	SUM
SRV_RESPONSE	COUNTER	False	Keeps track of the number of SRV responses received from the DNS server.	SUM

Column Name	Column Type	Index	Description	Aggregation Type
SRV_NO_ANS_RESPONSE	COUNTER	False	Keeps track of the number of SRV no answer responses.	SUM
SRV_REQUEST_TIMEOUT	COUNTER	False	Keeps track of the number of SRV request timeouts.	SUM
SRV_DEST_UNREACHABLE	COUNTER	False	Keeps track of the number of SRV destination unreachable counts.	SUM
A_REQUEST	COUNTER	False	Keeps track of the number of A requests sent to the DNS server.	SUM
A_RESPONSE	COUNTER	False	Keeps track of the number of A responses received from the DNS server.	SUM
A_NO_ANS_RESPONSE	COUNTER	False	Keeps track of the number of A no answer responses.	SUM
A_REQUEST_TIMEOUT	COUNTER	False	Keeps track of the number of A request timeouts.	SUM
A_DEST_UNREACHABLE	COUNTER	False	Keeps track of the number of A destination unreachable counts.	SUM
AAAA_REQUEST	COUNTER	False	Keeps track of the number of AAAA requests sent to the DNS server.	SUM
AAAA_RESPONSE	COUNTER	False	Keeps track of the number of AAAA responses received from the DNS server.	SUM
AAAA_NO_ANS_RESPONSE	COUNTER	False	Keeps track of the number of AAAA no answer responses.	SUM
AAAA_REQUEST_TIMEOUT	COUNTER	False	Keeps track of the number of AAAA request timeouts.	SUM
AAAA_DEST_UNREACHABLE	COUNTER	False	Keeps track of the number of AAAA destination unreachable counts.	SUM

Column Name	Column Type	Index	Description	Aggregation Type
TCP_CONNECTION_ATTEMPT	COUNTER	False	The number of TCP connection establishment attempts.	SUM
TCP_CONNECTION_ESTABLISH	COUNTER	False	The number of successfully established TCP connections.	SUM
TCP_CONNECTION_FAILED	COUNTER	False	The number of failed TCP connections.	SUM

SoftSwitchLwresdZoneStats

Column Name	Column Type	Index	Description	Aggregation Type
ZONE_NAME_LENGTH	INTEGER	True	Length of the Zone Name.	NA
ZONE_NAME	STRING	True	The ENUM Zone Name that the Counters apply to.	NA
NAPTR_REQUEST	COUNTER	False	Keeps track of the number of NAPTR requests sent to the ENUM zone.	SUM
NAPTR_RESPONSE	COUNTER	False	Keeps track of the number of NAPTR responses received from the ENUM zone.	SUM
NAPTR_NO_ANS_RESPONSE	COUNTER	False	Keeps track of the number of NAPTR no answer responses.	SUM
NAPTR_REQUEST_TIMEOUT	COUNTER	False	Keeps track of the number of NAPTR request timeouts.	SUM
NAPTR_DEST_UNREACHABLE	COUNTER	False	Keeps track of the number of NAPTR destination unreachable counts.	SUM
SRV_REQUEST	COUNTER	False	Keeps track of the number of SRV requests sent to the ENUM zone.	SUM

Column Name	Column Type	Index	Description	Aggregation Type
SRV_RESPONSE	COUNTER	False	Keeps track of the number of SRV responses received from the ENUM zone.	SUM
SRV_NO_ANS_RESPONSE	COUNTER	False	Keeps track of the number of SRV no answer responses.	SUM
SRV_REQUEST_TIMEOUT	COUNTER	False	Keeps track of the number of SRV request timeouts.	SUM
SRV_DEST_UNREACHABLE	COUNTER	False	Keeps track of the number of SRV destination unreachable counts.	SUM
A_REQUEST	COUNTER	False	Keeps track of the number of A requests sent to the ENUM zone.	SUM
A_RESPONSE	COUNTER	False	Keeps track of the number of A responses received from the ENUM zone.	SUM
A_NO_ANS_RESPONSE	COUNTER	False	Keeps track of the number of A no answer responses.	SUM
A_REQUEST_TIMEOUT	COUNTER	False	Keeps track of the number of A request timeouts.	SUM
A_DEST_UNREACHABLE	COUNTER	False	Keeps track of the number of A destination unreachable counts.	SUM
AAAA_REQUEST	COUNTER	False	Keeps track of the number of AAAA requests sent to the ENUM zone.	SUM
AAAA_RESPONSE	COUNTER	False	Keeps track of the number of AAAA responses received from the ENUM zone.	SUM
AAAA_NO_ANS_RESPONSE	COUNTER	False	Keeps track of the number of AAAA no answer responses.	SUM
AAAA_REQUEST_TIMEOUT	COUNTER	False	Keeps track of the number of AAAA request timeouts.	SUM

Column Name	Column Type	Index	Description	Aggregation Type
AAAA_DEST_UNREACHABLE	COUNTER	False	Keeps track of the number of AAAA destination unreachable counts.	SUM
TCP_CONNECTION_ATTEMPT	COUNTER	False	The number of TCP connection establishment attempts for the Zone.	SUM
TCP_CONNECTION_ESTABLISH	COUNTER	False	The number of successfully established TCP connections for the Zone.	SUM
TCP_CONNECTION_FAILED	INTEGER	False	The number of failed TCP connections for the Zone.	NA

SoftSwitchPesMWIServiceStats

Column Name	Column Type	Index	Description
SERVICE	COUNTER	No	Keeps tack of calls that execute MWI service
UPDATE_SERVICE	COUNTER	No	Keeps tack of calls that execute MWI Status Update service

SoftswitchScpa

SoftSwitchScpaAnsiTcStats

Column Name	Column Type	Index	Description
QUERY_SENT	COUNTER	No	Tracks the number of ANSI TCAP queries sent by the PSX.
QUERY_RCVD	COUNTER	No	Tracks the number of ANSI TCAP queries received by the PSX.
TIMEOUT	COUNTER	No	Tracks the number of ANSI TCAP queries that have timed out.

Column Name	Column Type	Index	Description
ERROR	COUNTER	No	Tracks the number of ANSI TCAP error messages received by the PSX.
PURGED	COUNTER	No	Tracks the number of ANSI TCAP queries purged by the PSX.
RSP_SENT	COUNTER	No	Tracks the number of ANSI TCAP responses sent by the PSX.
RSP_RCVD	COUNTER	No	Tracks the number of ANSI TCAP responses received by the PSX.
OPEN_TRANS	COUNTER	No	Tracks the number of ANSI TCAP transactions which are open pending a response.
DIALOG_ID_POOL_SIZE	COUNTER	No	Tracks the number of ANSI TCAP dialog ids allocated by the PSX/SGX.

SoftSwitchScpaGsmTcStats

Column Name	Column Type	Index	Description
QUERY_SENT	COUNTER	No	Tracks the number of GSM TCAP queries sent by the PSX
QUERY_RCVD	COUNTER	No	Tracks the number of GSM TCAP queries received by the PSX
TIMEOUT	COUNTER	No	Tracks the number of GSM TCAP queries that have timed out
ERROR	COUNTER	No	Tracks the number of GSM TCAP error messages received by the PSX
PURGED	COUNTER	No	Tracks the number of GSM TCAP queries purged by the PSX
RSP_SENT	COUNTER	No	Tracks the number of GSM TCAP responses sent by the PSX
RSP_RCVD	COUNTER	No	Tracks the number of GSM TCAP responses received by the PSX

Column Name	Column Type	Index	Description
OPEN_TRANS	COUNTER	No	Tracks the number of GSM TCAP transactions which are open pending a response
DIALOG_ID_POOL_SIZE	COUNTER	No	Tracks the number of GSM TCAP dialog ids allocated by the PSX/SGX

SoftSwitchScpaSpasStats

Note

SoftSwitchScpaSpasStats performance statistics table is not available on PSX versions 9.3 and later.

Column Name	Column Type	Index	Description
DEVICE_ID	STRING	Yes	The SPAS device name
START_DIALOG	COUNTER	No	Tracks the number of START_DLG messages sent by the PSX
END_DIALOG	COUNTER	No	Tracks the number of END_DLG messages sent by the PSX
ABORT_DIALOG	COUNTER	No	Tracks the number of ABRT_DLG messages sent/received by the PSX
SEND_CONFIRM	COUNTER	No	Tracks the number of SD_CNFRM messages received by the PSX
CONTINUE	COUNTER	No	Tracks the number of CONT messages received by the PSX
CONT_RSLT	COUNTER	No	Tracks the number of CONT_RSLT messages sent by the PSX
XFER	COUNTER	No	Tracks the number of XFER messages received by the PSX
XFER_RES	COUNTER	No	Tracks the number of XFER_RSLT messages sent by the PSX

Column Name	Column Type	Index	Description
XFER_TERM	COUNTER	No	Tracks the number of XFER_TERM messages sent by the PSX
CONT_TERM	COUNTER	No	Tracks the number of CONT_TERM messages sent by the PSX
RSET_CFNA	COUNTER	No	Tracks the number of RSET_CNFA messages received by the PSX
IGNORE	COUNTER	No	Tracks the number of IGNORE messages received by the PSX
RLS	COUNTER	No	Tracks the number of RLS messages received by the PSX
REG	COUNTER	No	Tracks the number of REG messages received by the PSX
REG_ACK	COUNTER	No	Tracks the number of REG_ACK messages sent by the PSX
KA_SENT	COUNTER	No	Tracks the number of KA messages sent by the PSX
KA_RCVD	COUNTER	No	Tracks the number of KA messages received by the PSX
KA_ACK_RCVD	COUNTER	No	Tracks the number of KA_ACK messages received by the PSX
KA_ACK_SENT	COUNTER	No	Tracks the number of KA_ACK messages sent by the PSX
TOTAL_MSG	COUNTER	No	Tracks the number of total messages counted in Round Trip Time (RTT) calculation
TOTAL_RTT	COUNTER64	No	This is the total Round Trip Time (RTT) in milliseconds
AVG_RTT	GAUGE	No	This is the average RTT value that is, $TOTAL\_RTT / TOTAL\_MSG$
SES_IN_PROG	GAUGE	No	Tracks the number of SPAS sessions in progress

SoftSwitchScpaTtcTcStats

Column Name	Column Type	Index	Description
QUERY_SENT	COUNTER	No	Tracks the number of TTC TCAP queries sent by the PSX
RETURN_SUCCESS	COUNTER	No	Tracks the number of TTC TCAP responses received successfully by the PSX
RETURN_ERROR	COUNTER	No	Tracks the number of TTC TCAP error messages received by the PSX
RETURN_ABORT	COUNTER	No	Tracks the number of TTC TCAP abort messages received by the PSX
UDTS_REPLIED	COUNTER	No	Tracks the number of TTC TCAP UDTS replies received by the PSX
RSP_TIMEOUT	COUNTER	No	Tracks the number of TTC TCAP queries timed out by the PSX

SoftswitchSipe

SoftSwitchSipeMiscStats

Column Name	Column Type	Index	Description
NUM_OF_GCED_CALLS	COUNTER	No	Tracks the number of transactions which have remained in the system for too long and have been removed by the Garbage Collector
GUARD_TIMER_CLR_CALLS	COUNTER	No	Tracks the number of transactions that are removed by Guard Timer Expiry

SoftSwitchSipeProxyReqSentStats

Column Name	Column Type	Index	Description
INVITE	COUNTER	No	Tracks the number of INVITE requests sent by the SIP process in proxy mode. Retransmissions of messages are not counted.
BYE	COUNTER	No	Tracks the number of BYE requests sent by the SIP process in proxy mode. Retransmissions of messages are not counted.
CANCEL	COUNTER	No	Tracks the number of CANCEL requests sent by the SIP process in proxy mode. Retransmissions of messages are not counted.
OPTIONS	COUNTER	No	Tracks the number of OPTIONS requests sent by the SIP process in proxy mode. Retransmissions of messages are not counted.
OTHER	COUNTER	No	Tracks the number of miscellaneous requests sent by the SIP process in proxy mode (and are not counted in specific counters). Retransmissions of messages (while the original one is being processed) are not counted.
REGISTER	COUNTER	No	Tracks the number of REGISTER requests sent by the SIP process in proxy mode. Retransmissions of messages are not counted.
SUBSCRIBE	COUNTER	No	Tracks the number of SUBSCRIBE requests sent by the SIP process in proxy mode. Retransmissions of messages are not counted.
NOTIFY	COUNTER	No	Tracks the number of NOTIFY requests sent by the SIP process in proxy mode. Retransmissions of messages are not counted.

Column Name	Column Type	Index	Description
RE_SENT_INVITE	COUNTER	No	Tracks the number of INVITE requests resent by the SIP process in proxy mode.
MESSAGE	COUNTER	No	Tracks the number of MESSAGE requests sent by the SIP process in proxy mode. Retransmissions of messages are not counted.

SoftSwitchSipeProxyRspRcvdStats

Column Name	Column Type	Index	Description
RSP_RCV_2XX	COUNTER	No	Tracks the number of 2XX responses received by the SIP process in proxy mode. Retransmissions of messages are not counted.
RSP_RCV_3XX	COUNTER	No	Tracks the number of 3XX responses received by the SIP process in proxy mode. Retransmissions of messages are not counted.
RSP_RCV_4XX	COUNTER	No	Tracks the number of 4XX responses received by the SIP process in proxy mode. Retransmissions of messages are not counted.
RSP_RCV_5XX	COUNTER	No	Tracks the number of 5XX responses received by the SIP process in proxy mode. Retransmissions of messages are not counted.
RSP_RCV_6XX	COUNTER	No	Tracks the number of 6XX responses received by the SIP process in proxy mode. Retransmissions of messages are not counted.

Column Name	Column Type	Index	Description
RCVD_NON_INV	COUNTER	No	Tracks the number of non INVITE responses received by the SIPE process in proxy mode.

SoftSwitchSipeProxyStats

Column Name	Column Type	Index	Description
LOCAL_RECUR_COUNTER	COUNTER	No	Tracks the number of times the local recursion service of SIPE proxy caused a final response to be handled locally, and another request was sent toward the next route in the route list.
TIMER_C	COUNTER	No	Tracks the number of times the SIPE proxy Timer C expired where the request is cancelled and a final response is sent back to the UAC.

SoftSwitchSipeReqRcvdStats

Column Name	Column Type	Index	Description
INVITE	COUNTER	No	Tracks the number of INVITE requests received by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.
BYE	COUNTER	No	Tracks the number of BYE requests received by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.
CANCEL	COUNTER	No	Tracks the number of INVITE requests received by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.

Column Name	Column Type	Index	Description
OPTIONS	COUNTER	No	Tracks the number of OPTIONS requests received by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.
OTHER	COUNTER	No	Tracks the number of miscellaneous requests received (and are not counted in specific counters) by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.
REGISTER	COUNTER	No	Tracks the number of REGISTER requests received by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.
SUBSCRIBE	COUNTER	No	Tracks the number of SUBSCRIBE requests received by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.
NOTIFY	COUNTER	No	Tracks the number of NOTIFY requests received by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.
NOTIFY_MWI_ON	COUNTER	No	Tracks the number of NOTIFY requests with MWI ON status, received by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.
NOTIFY_MWI_OFF	COUNTER	No	Tracks the number of NOTIFY requests with MWI OFF status, received by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.

Column Name	Column Type	Index	Description
NOTIFY_MWI_REG	COUNTER	No	Tracks the number of NOTIFY requests with Registration event, received by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.
INVITEWITH_ETS_RPH	COUNTER	No	Tracks the number of INVITE requests with ETS RPH, received by the SIP process. of messages (while the original one is being processed) are not counted.
INVITEWITH_ETS_DN	COUNTER	No	Tracks the number of INVITE requests with ETS DN but no ETS RPH, received by the SIP process. Retransmissions of messages (while the original one is being processed) are not counted.
RESP_WITH417_REASON	COUNTER	No	Tracks the number of 400 Response messages with 417 Reason Code received by the SIP process.
WITH_ETS_RPH_OVERLOAD	COUNTER	No	Tracks the number of requests with ETS RPH discarded due to overload.
WITHOUT_ETS_RPH_OVERLOAD	COUNTER	No	The counter keeps track of the number of Requests without ETS RPH discarded due to overload.
RCVD_CNAMESSUBSCRIBE	COUNTER	No	Tracks the number of SUBSCRIBE Requests for CNAME query. Event type - calling-name. Retransmissions are not counted.
MESSAGE	COUNTER	No	Tracks the number of MESSAGE requests received by the SIP process. Retransmissions of messages (while the original one is processing) are not counted.

SoftSwitchSipeRspSentStats

Column Name	Column Type	Index	Description
RSP_SENT_2XX	COUNTER	No	Tracks the number of 2XX responses sent by the SIP process. Retransmissions of messages are not counted.
RSP_SENT_3XX	COUNTER	No	Tracks the number of 3XX responses sent by the SIP process. Retransmissions of messages are not counted.
RSP_SENT_4XX	COUNTER	No	Tracks the number of 4XX responses sent by the SIP process. Retransmissions of messages are not counted.
RSP_SENT_5XX	COUNTER	No	Tracks the number of 5XX responses sent by the SIP process. Retransmissions of messages are not counted.
RSP_SENT_6XX	COUNTER	No	Tracks the number of 6XX responses sent by the SIP process. Retransmissions of messages are not counted.
SENT_NON_INVITE	COUNTER	No	Tracks the number of responses sent by the SIPE process in non INVITE transactions. Retransmissions of messages are not counted.
SENT_INVITE_WITH_ETSRPH	COUNTER	No	Tracks the number of INVITE requests sent with ETS RPH sent by the SIP process. Retransmissions of messages are not counted.

SoftSwitchSipeSumStats

Column Name	Column Type	Index	Description
AVG_TRANS_TIMER	GAUGE	No	This is the average time in milliseconds it took to process a SIPE request. - For Redirector, this is from the time a request is received to the time a 3XX is sent back. - For Proxy, this is from the time the request is received to the time the request is forwarded.
AVG_CALL_RATE	GAUGE	No	This is the average number of requests per second, which the SIPE is receiving.
TOTAL_REDIRECT_REQ	COUNTER	No	Tracks the number of redirected requests.
TOTAL_PROXY_REQ	COUNTER	No	Tracks the number of requests which were proxied. Requests that might otherwise be proxied but are rejected by routing (for example, no route found) are not counted.
PARSE_ERROR	COUNTER	No	Tracks the number of SIP Parse errors.
RETRANS_OTHER_MSG	COUNTER	No	Tracks the number of retransmitted messages other than INVITE.

TmCalling

TmCallingNumberAllowedStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
TMORIG_COUNTERS_ALLOWED_ENT	STRING	Yes	Entity ID (National Number) for origination with traffic control

Column Name	Column Type	Index	Description
TMORIG_COUNTERS_ALLOWED_ENT2	STRING	Yes	Entity ID2 (Country ID) for origination with traffic control
TMORIG_COUNTERS_ALLOWED_VALUE	COUNTER	No	The Number of allowed calls from origination with traffic control

TmCallingNumberBlockedStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
TMORIG_COUNTERS_BLOCKED_ENT	STRING	Yes	Entity ID (National Number) for origination with traffic control
TMORIG_COUNTERS_BLOCKED_ENT2	STRING	Yes	Entity ID2 (Country ID) for origination with traffic control
TMORIG_COUNTERS_BLOCKED_VALUE	COUNTER	No	The Number of blocked calls from origination with traffic control

TmDialed

TmDialedDestAllowedStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
TM_ENTITY	STRING	Yes	Entity Id (national number) for dialed destination with traffic control
TM_ENTITY2	STRING	Yes	Entity Id2 (country id) for dialed destination with traffic control
TM_VALUE	COUNTER	No	Number of allowed calls to dialed destination with traffic control

TmDialedDestBlockedStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
TM_ENTITY	STRING	Yes	Entity Id (national number) for dialed destination with traffic control
TM_ENTITY2	STRING	Yes	Entity Id2 (country id) for dialed destination with traffic control
TM_VALUE	COUNTER	No	Number of blocked calls to dialed destination with traffic control

TMFinal

TMFinalCallingNumAllowedStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
TM_ENTITY	STRING	Yes	Entity Id (trunk group id) for final calling number with traffic control
TM_ENTITY2	STRING	Yes	Entity Id2 (gateway id) for final calling number with traffic control
TM_VALUE	COUNTER	No	Number of allowed calls from final calling number with traffic control

TMFinalCallingNumBlockedStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
TM_ENTITY	STRING	Yes	Entity Id (trunk group id) for final calling number with traffic control
TM_ENTITY2	STRING	Yes	Entity Id2 (gateway id) for final calling number with traffic control
TM_VALUE	COUNTER	No	Number of blocked calls from final calling number with traffic control

TMFinalDestinationAllowedStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
TM_ENTITY	STRING	Yes	Entity Id (trunk group id) for final calling number with traffic control
TM_ENTITY2	STRING	Yes	Entity Id2 (gateway id) for final calling number with traffic control
TM_ENTITY_TYPE	INTEGER	Yes	Call Processing entity type to identify source of final destination allowed counter
TM_VALUE	COUNTER	No	Number of allowed calls from final calling number with traffic control

TMFinalDestinationBlockedStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
TM_ENTITY	STRING	Yes	Entity Id (trunk group id) for final calling number with traffic control
TM_ENTITY2	STRING	Yes	Entity Id2 (gateway id) for final calling number with traffic control
TM_ENTITY_TYPE	INTEGER	Yes	Call Processing entity type to identify source of final destination allowed counter
TM_VALUE	COUNTER	No	Number of blocked calls from final calling number with traffic control

TMTrans

TmTransDestAllowedStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
TM_ENTITY	STRING	Yes	Entity Id (national number) for translated destination with traffic control
TM_ENTITY2	STRING	Yes	Entity Id2 (country id) for translated destination with traffic control
TM_VALUE	COUNTER	No	Number of allowed calls to translated destination with traffic control

TmTransDestBlockedStats

Note

The performance statistics file is generated only if a traffic control profile is configured and the specified control type condition is triggered during an actual call.

For information on how to configure a Traffic Management profile, refer to [Traffic Control Application Screen](#).

Column Name	Column Type	Index	Description
TM_ENTITY	STRING	Yes	Entity Id (national number) for translated destination with traffic control
TM_ENTITY2	STRING	Yes	Entity Id2 (country id) for translated destination with traffic control
TM_VALUE	COUNTER	No	Number of blocked calls to translated destination with traffic control

TollFreeStats

Column Name	Column Type	Index	Description
TFC_NUM_REQUESTS	COUNTER	No	Number of requests that need Tollfree translation: Total number of requests received by the Ribbon SoftSwitch which require toll free translation.
TFC_NUM_REQUESTS_T O_SCP	COUNTER	No	Number of Toll free requests sent to SCP: Total number of requests sent to the SCP for translation.
TFC_NUM_REQUESTS_T RANSLATED	COUNTER	No	Number of Toll free requests translated: The number of toll free requests that were successfully translated.
TFC_NUM_REQUESTS_TI MED_OUT	COUNTER	No	Number of timed out toll free requests: Number of toll free requests that timed out.
TFC_NUM_REQUESTS_R EQ_ERRORS	COUNTER	No	Number of toll free request Errors: Number of toll free requests that resulted in an error.

SBC Core Statistics

The performance statistics supported for SBC Core are covered in this section.

- [MRFP Statistics](#)
- [SBC 5400 and SBC SWe Statistics](#)
- [SBC 7000 Statistics](#)
- [SBC CNF Statistics](#)
- [SLB Statistics](#)

MRFP Statistics

In this section:

- [CallCountIntervalStats](#)
- [CallCountIntervalStats_AG](#)
- [DspResDspCallIntervalStats](#)
- [DspResDspCallIntervalStats_AG](#)
- [DspResDspUsageIntervalStats](#)
- [DspResDspUsageIntervalStats_AG](#)

- EthernetPortMgmtStats
- EthernetPortPacketStats
- IcmpGeneralGroupStats
- IpAclOverallStats
- IpAclOverallStats_AG
- IpAclRuleStats
- IpAclRuleStats_AG
- IpGeneralGroupStats
- IpPolicingSystemIntStats
- IpPolicingSystemIntStats_AG
- LinkDetectionGroupStats
- LinkMonitorStats
- MRFPVmgGeneralIntStats
- MRFPVmgGeneralIntStats_AG
- MRFPVmgIpTermNotifyIntStats
- MRFPVmgIpTermNotifyIntStats_AG
- NBS5200CallCountStats
- NBS5200CallCountStats_AG
- SBX5KAclOffListIntStats
- SBX5KAggregateOffIntStats
- SBX5KArpOffListIntStats
- SBX5KBadEtherIpHdrOffIntStats
- SBX5KDiscardRuleOffIntStats
- SBX5KEthernetPortPacketPortStatus
- SBX5KLicenseUsageStats
- SBX5KMediaOffIntStats
- SBX5KRogueMediaIntStats
- SBX5KSystemDspStatusDspUsageStats
- SysCpuUtilIntStatsSts
- SysMemoryUtilIntStatsSts
- SystemCongestionIntervalStats
- SystemCongestionIntervalStats_AG
- SystemLicenseInfoStats
- UdpGeneralGroupStats

The following PM statistics tables are not supported for the MRFP:

- CallFailIntervalStats
- CallFailIntervalStats_AG
- CallIntervalStats
- CallIntervalStats_AG
- SBCCORESipIPPPresIntStats
- CORESipIPPPresIntStats_AG
- DnsGroupDnsServerStats
- H323SigPortStatisticsStats
- NBS5200TGStatusStats_AG
- NBS5200TrunkGroupStatusStats
- SBCCOREFacBlockingStats
- SBCCORESipIPPPresIntStats
- SBCCORESipRegCountDomIntStats
- SBCCORESipTGResIntStats
- SBCCORESipTGResIntStats_AG

- SBCCORETGAggregatedStats
- DiamNodeRfIntervalStatisticsStats
- SBX5KIpDecrOffIntStats
- SBX5KMtrmConnPortPeerStats
- RelayIntervalStatistics
- SBX5KSipByeResponseIntervalStats
- SBX5KSipInviteResponseIntervalStats
- SipOcsCallIntervalStats
- SBX5KSipOptResplntStats
- SBX5KSipRegResponseIntervalStats
- SBX5KSrtpDecryptOffIntStat
- SBX5KUflowOffListIntStats
- SBX5KDtlsSrtpStats
- SharedCacFailureIntStats
- SharedCacIntervalStatistics
- SipIntervalStats
- SipIntervalStats_AG
- SipRegCountStats
- SipRegCountStats_AG
- SipSigConnStatisticsStats
- SipSigPortStatisticsStats
- SipSigPortStatisticsStats_AG
- SipSubCountStats
- SipSubCountStats_AG
- TcpGeneralGroupStats
- TrafficControlStats
- ZoneIntervalStatisticsStats
- ZoneIntervalStatisticsStats_AG

In the following tables, rows that are colored red (as shown below) describe counters that are not applicable for MRFP. The CSV files are exported for these counters but with null values.

CallCountIntervalStats

Column Name	Column Type	Index	Description	canAggregate
NAME	INTEGER	True	This adds a dummy key to non-config scalar element container, even though only one row is allowed in container. Without the key, tailf treats the container non-dynamic and calls get_elem per leaf instead of calling get_object per row.	True
MAX_SESSION_COUNT	COUNTER	False	Displayed as maxSessionCallCount. The high watermark of total number of calls for the specified interval. This statistic accounts for calls that are stable.	True

Column Name	Column Type	Index	Description	canAggregate
MAX_POL_RTU_COUNT	INTEGER	False	Displays the same count as MAX_SESSION_COUNT if the SBC is using SBC-POL-RTU license. If the SBC is not using the SBC-POL-RTU license, the count is displayed as 0.	True
ENCRYPT_COUNT	COUNTER	False	Displayed as system wide total encrypt Call Count. The high watermark of total number of encrypt calls for the specified interval.	True
S RTP_COUNT	COUNTER	False	Displayed as system wide total Secure Real-time Transport Protocol (S RTP) Call Count; The high watermark of total number of S RTP calls for the specified interval.	True
VIDEO_COUNT	COUNTER	False	Displayed as system wide total video Call Count. The high watermark of total number of video calls for the specified interval.	True
AMRNB_COUNT	COUNTER	False	The high watermark of total number of Adaptive Multi-Rate Narrowband (AMRNB) calls for the specified interval	True
AMRWB_COUNT	COUNTER	False	The high watermark of total number of Adaptive Multi-Rate Wideband (AMRWB) calls for the specified interval	True
EVRC_COUNT	COUNTER	False	The high watermark of total number of Enhanced Variable Rate Codec (EVRC) calls for the specified interval	True
NICEREC_COUNT	COUNTER	False	The current high watermark of total number of NICE recording calls	True
MRFSESS_COUNT	COUNTER	False	The current high watermark of total number of Media Resource Function (MRF) calls	True

Column Name	Column Type	Index	Description	canAggregate
MAX_PSX_RTU_COUNT	INTEGER	False	Displays MAX_SESSION_COUNT when the SBC is using the SBC-PSX-RTU license. If the SBC is not using SBC-PSX-RTU license it displays the count as 0.	True
VDSPRTU_COUNT	COUNTER	False	The high watermark of total number of trans-coded sessions for the specified interval	True
PDCS_COUNT	COUNTER	False	The high watermark of total number of pdcs header sessions for the specified interval	True
SIPREC_COUNT	COUNTER	False	The current high watermark of total number of sip recording calls	True
LI_ENABLED	INTEGER	False	Set based on whether LI license is available at the SBC	True
DSPG722_ENABLED	INTEGER	False	Set based on whether DspG722 license is available at the SBC	True
GMP4X1_ENABLED	INTEGER	False	Set based on whether 4X1GMP license is available at the SBC	True
SIPI_ENABLED	INTEGER	False	Set based on whether Sipi license is available at the SBC	True
SIP323_ENABLED	INTEGER	False	Set based on whether SipRec license is available at the SBC	True
GMP1X10_ENABLED	INTEGER	False	Set based on whether 1X10GMP license is available at the SBC	True
CAPACITY_ENABLED	INTEGER	False	Set based on whether Capacity license is available at the SBC	True
E911_ENABLED	INTEGER	False	Set based on whether E911 license is available at the SBC	True
ENUM_ENABLED	INTEGER	False	Set based on whether ENUM license is available at the SBC	True

Column Name	Column Type	Index	Description	canAggregate
SWINSTANCE_ENABLED	INTEGER	False	Set based on whether Swe Instance license is available at the SBC	True
EVS_COUNT	COUNT	False	The high watermark of total number of Enhanced Voice Services (EVS) calls for the specified interval	True
SILK_COUNT	COUNT	False	The high watermark of total number of SILK Codec Transcode calls for the specified interval	True
SBCRCS_COUNT	COUNT	False	The high watermark of total number of OOD calls that use an RCS based service for the specified interval	True
HPC_QUE_ATTEMPT	COUNT	No	The number of HPC calls successfully placed on HPC Call Queuing queues for the reporting interval	True
SLBSESS_COUNT	COUNT	No	Displayed as system wide total stable SLB sessions Count. The high watermark of the total number of active calls for the reporting interval.	True
LBINSTANCE_ENABLED	INTEGER	No	Set based on whether SLB license is available at the SLB	False
HPC_QUE_OVERFLOW	COUNT	No	The number of HPC calls which experienced unsuccessful call queuing attempts due to full queues for the reporting interval	True
HPC_QUE_ABANDON	COUNT	No	The number of queued HPC calls abandoned before call completion during the reporting interval	True
HPC_QUE_TIMEOUTS	COUNT	No	The number of HPC calls removed from the queue due to expiration of the queue timeout timer for the reporting interval	True
HPC_CTL_TFC_EXEM	COUNT	No	The HPC traffic control exemptions for this reporting interval	True

Column Name	Column Type	Index	Description	canAggregate
SOSBC_RTU_COUNT	COUNTER	False	The system wide total stable SOSBC sessions count. The high water mark of total number of active calls for the reporting interval.	True
WEB_SOCKET_COUNT	COUNTER	False	The high water mark of total number of web socket calls for this reporting interval	True
CE_NAME	STRING	False	The name of the compute element for this entry	False

CallCountIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate
NAME	INTEGER	True	This adds a dummy key to non-config scalar element container, even though only one row is allowed in container. Without the key, tailf treats the container non-dynamic and calls get_elem per leaf instead of calling get_object per row.	True
MAX_SESSION_COUNT	COUNTER	False	Displayed as maxSessionCallCount. The high watermark of total number of calls for the specified interval. This statistic accounts for calls that are stable.	True
MAX_POL_RTU_COUNT	INTEGER	False	Displays the same count as MAX_SESSION_COUNT if the SBC is using SBC-POL-RTU license. If the SBC is not using the SBC-POL-RTU license, the count is displayed as 0.	True
ENCRYPT_COUNT	COUNTER	False	Displayed as system wide total encrypt Call Count. The high watermark of total number of encrypt calls for the specified interval.	True

Column Name	Column Type	Index	Description	canAggregate
SRTP_COUNT	COUNTER	False	Displayed as system wide total Secure Real-time Transport Protocol (SRTP) Call Count; The high watermark of total number of SRTP calls for the specified interval.	True
VIDEO_COUNT	COUNTER	False	Displayed as system wide total video Call Count; The high watermark of total number of video calls for the specified interval.	True
AMRNB_COUNT	COUNTER	False	The high watermark of total number of Adaptive Multi-Rate Narrowband (AMRNB) calls for the specified interval.	True
AMRWB_COUNT	COUNTER	False	The high watermark of total number of Adaptive Multi-Rate Wideband (AMRWB) calls for the specified interval.	True
EVRC_COUNT	COUNTER	False	The high watermark of total number of Enhanced Variable Rate Codec (EVRC) calls for the specified interval.	True
NICEREC_COUNT	COUNTER	False	The current high watermark of total number of NICE recording calls.	True
MRFSESS_COUNT	COUNTER	False	The current high watermark of total number of Media Resource Function (MRF) calls.	True
MAX_PSX_RTU_COUNT	INTEGER	False	Displays MAX_SESSION_COUNT when the SBC is using the SBC-PSX-RTU license. If the SBC is not using SBC-PSX-RTU license it displays the count as 0.	True
VDSPRTU_COUNT	COUNTER	False	The high watermark of total number of trans-coded sessions for the specified interval.	True
PDCS_COUNT	COUNTER	False	The high watermark of total number of pdcS header sessions for the specified interval.	True

Column Name	Column Type	Index	Description	canAggregate
SIPREC_COUNT	COUNTER	False	The current high watermark of total number of sip recording calls.	True
LI_ENABLED	INTEGER	False	Set based on whether LI license is available at the SBC.	True
DSPG722_ENABLED	INTEGER	False	Set based on whether DspG722 license is available at the SBC.	True
GMP4X1_ENABLED	INTEGER	False	Set based on whether 4X1GMP license is available at the SBC.	True
SIPI_ENABLED	INTEGER	False	Set based on whether Sipi license is available at the SBC.	True
SIP323_ENABLED	INTEGER	False	Set based on whether SipRec license is available at the SBC.	True
GMP1X10_ENABLED	INTEGER	False	Set based on whether 1X10GMP license is available at the SBC.	True
CAPACITY_ENABLED	INTEGER	False	Set based on whether Capacity license is available at the SBC.	True
E911_ENABLED	INTEGER	False	Set based on whether E911 license is available at the SBC.	True
ENUM_ENABLED	INTEGER	False	Set based on whether ENUM license is available at the SBC.	True
SWINSTANCE_ENABLED	INTEGER	False	Set based on whether Swe Instance license is available at the SBC.	True
EVS_COUNT	COUNT	False	The high watermark of total number of Enhanced Voice Services (EVS) calls for the specified interval.	True
SILK_COUNT	COUNT	False	The high watermark of total number of SILK Codec Transcode calls for the specified interval.	True
SBCRCS_COUNT	COUNT	False	The high watermark of total number of OOD calls that use an RCS based service for the specified interval.	True

Column Name	Column Type	Index	Description	canAggregate
HPC_QUE_ATTEMPT	COUNT	No	The number of HPC calls successfully placed on HPC Call Queuing queues for the reporting interval.	True
SLBSESS_COUNT	COUNT	No	Displayed as system wide total stable SLB sessions Count. The high watermark of the total number of active calls for the reporting interval.	True
LBINSTANCE_ENABLED	INTEGER	No	Set based on whether SLB license is available at the SLB.	False
HPC_QUE_OVERFLOW	COUNT	No	The number of HPC calls which experienced unsuccessful call queuing attempts due to full queues for the reporting interval.	True
HPC_QUE_ABANDON	COUNT	No	The number of queued HPC calls abandoned before call completion during the reporting interval.	True
HPC_QUE_TIMEOUTS	COUNT	No	The number of HPC calls removed from the queue due to expiration of the queue timeout timer for the reporting interval.	True
HPC_CTL_TFC_EXEM	COUNT	No	The HPC traffic control exemptions for this reporting interval.	True
SOSBC_RTU_COUNT	COUNTER	False	The system wide total stable SOSBC sessions count. The high water mark of total number of active calls for the reporting interval.	True
WEB_SOCKET_COUNT	COUNTER	False	The high water mark of total number of web socket calls for this reporting interval.	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

DspResDspCallIntervalStats

Column Name	Type	Index	Description	canAggregate
SYSTEM_NAME	STRING	True	The name of the system	False
NUM_CALL_NO_DSP_ALLOC_FAIL	COUNTER	False	The count of successful calls without DSP resource allocation failure during an interval time	True
NUM_CALL_WITH_DSP_ALLOC_FAIL	COUNTER	False	The count of successful calls with DSP resource allocation failure during an interval time	True
NUM_CALL_FAIL_NO_G729	COUNTER	False	The count of calls failed due to lack of G729 DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_ON_G729	COUNTER	False	The count of calls failed due to reasons other than lack G729 DSP resource during an interval time	True
NUM_CALL_SUCCESS_NO_G729	COUNTER	False	The count of successful calls even with the lack of G729 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_G726	COUNTER	False	The count of calls failed due to lack of G726 DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_ON_G726	COUNTER	False	The count of calls failed due to reasons other than lack G726 DSP resource during an interval time	True
NUM_CALL_SUCCESS_NO_G726	COUNTER	False	The count of successful calls even with the lack of G726 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_G711_PACKET	COUNTER	False	The count of calls failed due to lack of G711 Packet DSP resource during an interval time	True
NUM_CALL_FAIL_ON_G711_PACKET	COUNTER	False	The count of calls failed due to reasons other than lack G711 Packet DSP resource during an interval time	True

Column Name	Type	Index	Description	canAggregate
NUM_CALL_NO_G711_PACKET	COUNTER	False	Number of call was successful even with the lack of G711 Packet DSP resource during an interval time	True
NUM_CALL_FAIL_NO_G723	COUNTER	False	Number of call failed due to lack of G723 DSP resource during an interval time	True
NUM_CALL_FAIL_ON_G723	COUNTER	False	The count of calls failed due to reasonss other than lack G723 DSP resource during an interval time	True
NUM_CALL_NO_G723	COUNTER	False	Number of call was successful even with the lack of G723 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_ILBC	COUNTER	False	Number of call failed due to lack of ILBC DSP resource during an interval time	True
NUM_CALL_FAIL_ON_ILBC	COUNTER	False	The count of calls failed due to reasonss other than lack ILBC DSP resource during an interval time	True
NUM_CALL_NO_ILBC	COUNTER	False	Number of call was successful even with the lack of ILBC DSP resource during an interval time	True
NUM_CALL_FAIL_NO_EVRCB	COUNTER	False	Number of call failed due to lack of EVRCB0 DSP resource during an interval time	True
NUM_CALL_FAIL_ON_EVRCB	COUNTER	False	The count of calls failed due to reasonss other than lack EVRCB0 DSP resource during an interval time	True
NUM_CALL_NO_EVRCB	COUNTER	False	Number of call was successful even with the lack of EVRCB0 DSP resource during an interval time	True

Column Name	Type	Index	Description	canAggregate
NUM_CALL_FAIL_NO_GSM	COUNTER	False	Number of call failed due to lack of AMRNB DSP resource during an interval time	True
NUM_CALL_FAIL_ON_GSM	COUNTER	False	The count of calls failed due to reasonss other than lack AMRNB DSP resource during an interval time	True
NUM_CALL_NO_GSM	COUNTER	False	Number of call was successful even with the lack of AMRNB DSP resource during an interval time	True
NUM_CALL_FAIL_NO_AMRWB	COUNTER	False	Number of call failed due to lack of AMRWB DSP resource during an interval time	True
NUM_CALL_FAIL_ON_AMRWB	COUNTER	False	The count of calls failed due to reasonss other than lack AMRWB DSP resource during an interval time	True
NUM_CALL_NO_AMRWB	COUNTER	False	Number of call was successful even with the lack of AMRWB DSP resource during an interval time	True
NUM_CALL_FAIL_NO_G722	COUNTER	False	Number of call failed due to lack of G722 DSP resource during an interval time	True
NUM_CALL_FAIL_ON_G722	COUNTER	False	The count of calls failed due to reasonss other than lack G722 DSP resource during an interval time	True
NUM_CALL_NO_G722	COUNTER	False	Number of call was successful even with the lack of G722 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_TONE	COUNTER	False	Number of call failed due to lack of TONE DSP resource during an interval time	True

Column Name	Type	Index	Description	canAggregate
NUM_CALL_FAIL_ON_TONE	COUNTER	False	The count of calls failed due to reasons other than lack TONE DSP resource during an interval time	True
NUM_CALL_NO_TONE	COUNTER	False	Number of call was successful even with the lack of TONE DSP resource during an interval time	True
NUM_CALL_FAIL_NO_EVRC	COUNTER	False	Number of call failed due to lack of EVRC DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_ON_EVRC	COUNTER	False	The count of calls failed due to reasons other than lack EVRC DSP resource during an interval time	True
NUM_CALL_SUCCESS_NO_EVRC	COUNTER	False	Number of call was successful even with the lack of EVRC DSP resource during an interval time	True
NUM_CALL_FAIL_NO_G7221	COUNTER	False	Number of call failed due to lack of G7221 DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_ON_G7221	COUNTER	False	The count of calls failed due to reasons other than lack G7221 DSP resource during an interval time	True
NUM_CALL_SUCCESS_NO_G7221	COUNTER	False	Number of call was successful even with lack of G7221 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_EFR	COUNTER	False	Number of call failed due to lack of Efr DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_ON_EFR	COUNTER	False	The count of calls failed due to reasons other than lack Efr DSP resource during an interval time	True
NUM_CALL_SUCCESS_NO_EFR	COUNTER	False	Number of call was successful even with the lack of Efr DSP resource during an interval time	True

Column Name	Type	Index	Description	canAggregate
NUM_CALL_FAIL_NO_OPUS	COUNTER	False	Number of call failed due to lack of OPUS DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_ON_OPUS	COUNTER	False	The count of calls failed due to reasons other than lack of OPUS DSP resource during an interval time	True
NUM_CALL_SUCCESSES_NO_OPUS	COUNTER	False	Number of call was successful even with the lack of OPUS DSP resource during an interval time	True
NUM_CALL_FAIL_NO_EVS	COUNTER	False	Number of call failed due to lack of EVS DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_EVS	COUNTER	False	The count of calls failed due to reasons other than lack of EVS DSP resource during an interval time	True
NUM_CALL_SUCCESSES_NO_EVS	COUNTER	False	Number of call was successful even with the lack of EVS DSP resource during an interval time	True
NUM_CALL_FAIL_NO_SILK8	COUNTER	False	Number of call failed due to lack of SILK8 DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_SILK8	COUNTER	False	The count of calls failed due to reasons other than lack of SILK8 DSP resource during an interval time	True
NUM_CALL_SUCCESSES_NO_SILK8	COUNTER	False	Number of call was successful even with the lack of SILK8 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_SILK16	COUNTER	False	Number of call failed due to lack of SILK16 DSP resource during an interval time	True

Column Name	Type	Index	Description	canAggregate
NUM_CALL_FAIL_OTHER_SILK16	COUNTER	False	The count of calls failed due to reasons other than lack of SILK16 DSP resource during an interval time	True
NUM_CALL_SUCCESS_NO_SILK16	COUNTER	False	Number of call was successful even with the lack of SILK16 DSP resource during an interval time	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

DspResDspCallIntervalStats_AG

Column Name	Type	Index	Description	canAggregate
SYSTEM_NAME	STRING	True	Name of the system.	False
NUM_CALL_NO_DSP_ALLOC_FAIL	COUNTER	False	Number of call was successful without DSP resource allocation failure during an interval time	True
NUM_CALL_WITH_DSP_ALLOC_FAIL	COUNTER	False	Number of call was successful with DSP resource allocation failure during an interval time	True
NUM_CALL_FAIL_NO_G729	COUNTER	False	Number of call failed due to lack of G729 DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_ON_G729	COUNTER	False	The count of calls failed due to reasons other than lack G729 DSP resource during an interval time	True
NUM_CALL_SUCCESS_NO_G729	COUNTER	False	Number of call was successful even with the lack of G729 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_G726	COUNTER	False	Number of call failed due to lack of G726 DSP resource during an interval time	True

Column Name	Type	Index	Description	canAggregate
NUM_CALL_FAIL_OTHER_ON_G726	COUNTER	False	The count of calls failed due to reasons other than lack G726 DSP resource during an interval time	True
NUM_CALL_SUCCESS_NO_G726	COUNTER	False	Number of call was successful even with the lack of G726 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_G711_PACKET	COUNTER	False	Number of call failed due to lack of G711 Packet DSP resource during an interval time	True
NUM_CALL_FAIL_ON_G711_PACKET	COUNTER	False	The count of calls failed due to reasons other than lack G711 Packet DSP resource during an interval time	True
NUM_CALL_NO_G711_PACKET	COUNTER	False	Number of call was successful even with the lack of G711 Packet DSP resource during an interval time	True
NUM_CALL_FAIL_NO_G723	COUNTER	False	Number of call failed due to lack of G723 DSP resource during an interval time	True
NUM_CALL_FAIL_ON_G723	COUNTER	False	The count of calls failed due to reasons other than lack G723 DSP resource during an interval time	True
NUM_CALL_NO_G723	COUNTER	False	Number of call was successful even with the lack of G723 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_ILBC	COUNTER	False	Number of call failed due to lack of ILBC DSP resource during an interval time	True
NUM_CALL_FAIL_ON_ILBC	COUNTER	False	The count of calls failed due to reasons other than lack ILBC DSP resource during an interval time	True

Column Name	Type	Index	Description	canAggregate
NUM_CALL_NO_ILBC	COUNTER	False	Number of call was successful even with the lack of ILBC DSP resource during an interval time	True
NUM_CALL_FAIL_NO_EVR CB	COUNTER	False	Number of call failed due to lack of EVRCB0 DSP resource during an interval time	True
NUM_CALL_FAIL_ON_EVR CB	COUNTER	False	The count of calls failed due to reasons other than lack EVRCB0 DSP resource during an interval time	True
NUM_CALL_NO_EVR CB	COUNTER	False	Number of call was successful even with the lack of EVRCB0 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_GSM	COUNTER	False	Number of call failed due to lack of AMRNB DSP resource during an interval time	True
NUM_CALL_FAIL_ON_GSM	COUNTER	False	The count of calls failed due to reasons other than lack AMRNB DSP resource during an interval time	True
NUM_CALL_NO_GSM	COUNTER	False	Number of call was successful even with the lack of AMRNB DSP resource during an interval time	True
NUM_CALL_FAIL_NO_AMRWB	COUNTER	False	Number of call failed due to lack of AMRWB DSP resource during an interval time	True
NUM_CALL_FAIL_ON_AMRWB	COUNTER	False	The count of calls failed due to reasons other than lack AMRWB DSP resource during an interval time	True
NUM_CALL_NO_AMR WB	COUNTER	False	Number of call was successful even with the lack of AMRWB DSP resource during an interval time	True

Column Name	Type	Index	Description	canAggregate
NUM_CALL_FAIL_NO_G722	COUNTER	False	Number of call failed due to lack of G722 DSP resource during an interval time	True
NUM_CALL_FAIL_ON_G722	COUNTER	False	The count of calls failed due to reasons other than lack G722 DSP resource during an interval time	True
NUM_CALL_NO_G722	COUNTER	False	Number of call was successful even with the lack of G722 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_TONE	COUNTER	False	Number of call failed due to lack of TONE DSP resource during an interval time	True
NUM_CALL_FAIL_ON_TONE	COUNTER	False	The count of calls failed due to reasons other than lack TONE DSP resource during an interval time	True
NUM_CALL_NO_TONE	COUNTER	False	Number of call was successful even with the lack of TONE DSP resource during an interval time	True
NUM_CALL_FAIL_NO_EVRC	COUNTER	False	Number of call failed due to lack of EVRC DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_ON_EVRC	COUNTER	False	The count of calls failed due to reasons other than lack EVRC DSP resource during an interval time	True
NUM_CALL_SUCCESS_NO_EVRC	COUNTER	False	Number of call was successful even with the lack of EVRC DSP resource during an interval time	True
NUM_CALL_FAIL_NO_G7221	COUNTER	False	Number of call failed due to lack of G7221 DSP resource during an interval time	True

Column Name	Type	Index	Description	canAggregate
NUM_CALL_FAIL_OT HER_ON_G7221	COUNTER	False	The count of calls failed due to reasons other than lack G7221 DSP resource during an interval time	True
NUM_CALL_SUCCES S_NO_G7221	COUNTER	False	Number of call was successful even with lack of G7221 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_ EFR	COUNTER	False	Number of call failed due to lack of Efr DSP resource during an interval time	True
NUM_CALL_FAIL_OT HER_ON_EFR	COUNTER	False	The count of calls failed due to reasons other than lack Efr DSP resource during an interval time	True
NUM_CALL_SUCCES S_NO_EFR	COUNTER	False	Number of call was successful even with the lack of Efr DSP resource during an interval time	True
NUM_CALL_FAIL_NO_ OPUS	COUNTER	False	Number of call failed due to lack of OPUS DSP resource during an interval time	True
NUM_CALL_FAIL_OT HER_ON_OPUS	COUNTER	False	The count of calls failed due to reasons other than lack of OPUS DSP resource during an interval time	True
NUM_CALL_SUCCES S_NO_OPUS	COUNTER	False	Number of call was successful even with the lack of OPUS DSP resource during an interval time	True
NUM_CALL_FAIL_NO_ EVS	COUNTER	False	Number of call failed due to lack of EVS DSP resource during an interval time	True
NUM_CALL_FAIL_OT HER_EVS	COUNTER	False	The count of calls failed due to reasons other than lack of EVS DSP resource during an interval time	True
NUM_CALL_SUCCES S_NO_EVS	COUNTER	False	Number of call was successful even with the lack of EVS DSP resource during an interval time	True

Column Name	Type	Index	Description	canAggregate
NUM_CALL_FAIL_NO_SILK8	COUNTER	False	Number of call failed due to lack of SILK8 DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_SILK8	COUNTER	False	The count of calls failed due to reasons other than lack of SILK8 DSP resource during an interval time	True
NUM_CALL_SUCCESS_NO_SILK8	COUNTER	False	Number of call was successful even with the lack of SILK8 DSP resource during an interval time	True
NUM_CALL_FAIL_NO_SILK16	COUNTER	False	Number of call failed due to lack of SILK16 DSP resource during an interval time	True
NUM_CALL_FAIL_OTHER_SILK16	COUNTER	False	The count of calls failed due to reasons other than lack of SILK16 DSP resource during an interval time	True
NUM_CALL_SUCCESS_NO_SILK16	COUNTER	False	Number of call was successful even with the lack of SILK16 DSP resource during an interval time	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

DspResDspUsageIntervalStats

Column Name	Type	Index	Description	canAggregate
SYSTEM_NAME	STRING	True	Name of the system.	False
G729_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G729 DSP pad during an interval time	True
G729_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G729 DSP pad during an interval time	True
G729_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G729 DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
G726_PEAK_USED_COUNT	GAUGE	False	The interval number of Peak usage of type G726 DSP pad during an interval time	True
G726_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G726 DSP pad during an interval time	True
G726_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G726 DSP pad during an interval time	True
G711_PACKET_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G711Packet DSP pad during an interval time	True
G711_PACKET_AVG_USED_COUNT	GAUGE	False	The average usage of type G711Packet DSP pad during an interval time	True
G711_PACKET_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type G711Packet DSP pad during an interval time	True
G723_PEAK_USED_COUNT	GAUGE	False	The interval number of Peak usage of type G723 DSP pad during an interval time	True
G723_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G723 DSP pad during an interval time	True
G723_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G723 DSP pad during an interval time	True
ILBC_PEAK_USED_COUNT	GAUGE	False	The peak usage of type ILBC DSP pad during an interval time	True
ILBC_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type ILBC DSP pad during an interval time	True
ILBC_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type ILBC DSP pad during an interval time	True
EVRCB0_PEAK_USED_COUNT	GAUGE	False	The peak usage of type EVRCB0 DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
EVRCB0_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type EVRCB0 DSP pad during an interval time	True
EVRCB0_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type EVRCB0 DSP pad during an interval time	True
GSM_PEAK_USED_COUNT	GAUGE	False	The peak usage of type AMRNB DSP pad during an interval time	True
GSM_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type AMRNB DSP pad during an interval time	True
GSM_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type AMRNB DSP pad during an interval time	True
AMRWB_PEAK_USED_COUNT	GAUGE	False	The peak usage of type Amrwb DSP pad during an interval time	True
AMRWB_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type Amrwb DSP pad during an interval time	True
AMRWB_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type Amrwb DSP pad during an interval time	True
G722_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G722 DSP pad during an interval time	True
G722_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G722 DSP pad during an interval time	True
G722_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G722 DSP pad during an interval time	True
TONE_PEAK_USED_COUNT	GAUGE	False	The peak usage of type TONE DSP pad during an interval time	True
TONE_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type TONE DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
TONE_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type TONE DSP pad during an interval time	True
EVRC_PEAK_USED_COUNT	GAUGE	False	The peak usage of type EVRCB0 DSP pad during an interval time	True
EVRC_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type EVRC DSP pad during an interval time	True
EVRC_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type EVRC DSP pad during an interval time	True
G7221_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G7221 DSP pad during an interval time	True
G7221_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G7221 DSP pad during an interval time	True
G7221_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G7221 DSP pad during an interval time	True
EFR_PEAK_USED_COUNT	GAUGE	False	The peak usage of type Efr DSP pad during an interval time	True
EFR_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type Efr DSP pad during an interval time	True
EFR_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type Efr DSP pad during an interval time	True
G711SS_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G711Ss DSP pad during an interval time	True
G711SS_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G711Ss DSP pad during an interval time	True
G711SS_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G711Ss DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
G729V8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G729 V8 DSP pad during an interval time	True
G729V8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G729 V8 DSP pad during an interval time	True
G729V8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G729 V8 DSP pad during an interval time	True
G726V8_PEAK_USED_COUNT	GAUGE	False	The interval number of Peak usage of type G726 V8 DSP pad during an interval time	True
G726V8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G726 V8 DSP pad during an interval time	True
G726V8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G726 V8 DSP pad during an interval time	True
G711V8_PACKET_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G711Packet V8 DSP pad during an interval time	True
G711V8_PACKET_AVG_USED_COUNT	GAUGE	False	The average usage of type G711Packet V8 DSP pad during an interval time	True
G711V8_PACKET_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type G711Packet V8 DSP pad during an interval time	True
G711SSV8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G711SSPacket V8 DSP pad during an interval time	True
G711SSV8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G711SSPacket V8 DSP pad during an interval time	True
G711SSV8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G711SSPacket V8 DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
G723V8_PEAK_USED_COUNT	GAUGE	False	The interval number of Peak usage of type G723 V8 DSP pad during an interval time	True
G723V8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G723 V8 DSP pad during an interval time	True
G723V8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G723 V8 DSP pad during an interval time	True
ILBCV8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type ILBC V8 DSP pad during an interval time	True
ILBCV8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type ILBC V8 DSP pad during an interval time	True
ILBCV8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type ILBC V8 DSP pad during an interval time	True
G722V8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G722 V8 DSP pad during an interval time	True
G722V8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G722 V8 DSP pad during an interval time	True
G722V8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G722 V8 DSP pad during an interval time	True
G7221V8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G722.1 V8 DSP pad during an interval time	True
G7221V8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G722.1 V8 DSP pad during an interval time	True
G7221V8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G722.1 V8 DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
OPUS_PEAK_USED_COUNT	GAUGE	False	The peak usage of type OPUS DSP pad during an interval time	True
OPUS_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type OPUS DSP pad during an interval time	True
OPUS_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type OPUS DSP pad during an interval time	True
EVS_PEAK_USED_COUNT	GAUGE	False	The peak usage of type EVS DSP pad during an interval time	True
EVS_AVG_USED_COUNT	GAUGE	False	The average usage of type EVS DSP pad during an interval time	True
EVS_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type EVS DSP pad during an interval time	True
SILK8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type SILK8 DSP pad during an interval time	True
SILK8_AVG_USED_COUNT	GAUGE	False	The average usage of type SILK8 DSP pad during an interval time	True
SILK8_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type SILK8 DSP pad during an interval time	True
SILK16_PEAK_USED_COUNT	GAUGE	False	The peak usage of type SILK16 DSP pad during an interval time	True
SILK16_AVG_USED_COUNT	GAUGE	False	The average usage of type SILK16 DSP pad during an interval time	True
SILK16_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type SILK16 DSP pad during an interval time	True
AMRWT140_PEAK_USED_COUNT	GAUGE	False	The peak usage of type AMR with T140 DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
AMRWT140_AVG_USED_COUNT	GAUGE	False	The average usage of type AMR with T140 DSP pad during an interval time	True
AMRWT140_AVG_AVAILABLE_COUNT	GAUGE	False	The average availability of type AMR with T140 DSP pad during an interval time	True
AMRWBT140_PEAK_USED_COUNT	GAUGE	False	The peak usage of type AMR-WB with T140 DSP pad during an interval time	True
AMRWBT140_AVG_USED_COUNT	GAUGE	False	The average usage of type AMR-WB with T140 DSP pad during an interval time	True
AMRWBT140_AVG_AVAILABLE_COUNT	GAUGE	False	The average availability of type AMR-WB with T140 DSP pad during an interval time	True
G711_WITHOUT_XCODE_RES_PEAK_COUNT	GAUGE	False	The peak count (during the interval time) of G.711 legs (terminations) that did not require a DSP resource The processing for the G.711 leg is done by the DSP resource allocated for the other leg in the call.	True
G711_WITHOUT_XCODE_RES_AVG_COUNT	GAUGE	False	The average count (during the interval time) of G.711 legs (terminations) that did not require a DSP resource The processing for the G.711 leg is done by the DSP resource allocated for the other leg in the call.	True
EVS_T140_PEAK_USED_COUNT	GAUGE	False	The peak usage of type EVS with T.140 DSP pad during an interval time	False
EVS_T140_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type EVS with T.140 DSP pad during an interval time	False

Column Name	Type	Index	Description	canAggregate
EVS_T140_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type EVS with T.140 DSP pad during an interval time	False
CE_NAME	STRING	False	The name of the compute element for this entry	False

DspResDspUsageIntervalStats_AG

Column Name	Type	Index	Description	canAggregate
SYSTEM_NAME	STRING	True	Name of the system	False
G729_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G729 DSP pad during an interval time	True
G729_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G729 DSP pad during an interval time	True
G729_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G729 DSP pad during an interval time	True
G726_PEAK_USED_COUNT	GAUGE	False	The interval number of Peak usage of type G726 DSP pad during an interval time	True
G726_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G726 DSP pad during an interval time	True
G726_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G726 DSP pad during an interval time	True
G711_PACKET_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G711Packet DSP pad during an interval time	True
G711_PACKET_AVG_USED_COUNT	GAUGE	False	The average usage of type G711Packet DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
G711_PACKET_AVG_A VAIL_COUNT	GAUGE	False	The average availability of type G711Packet DSP pad during an interval time	True
G723_PEAK_USED_C OUNT	GAUGE	False	The interval number of Peak usage of type G723 DSP pad during an interval time	True
G723_AVERAGE_USE D_COUNT	GAUGE	False	The average usage of type G723 DSP pad during an interval time	True
G723_AVERAGE_AVAIL _COUNT	GAUGE	False	The average availability of type G723 DSP pad during an interval time	True
ILBC_PEAK_USED_CO UNT	GAUGE	False	The peak usage of type ILBC DSP pad during an interval time	True
ILBC_AVERAGE_USED _COUNT	GAUGE	False	The average usage of type ILBC DSP pad during an interval time	True
ILBC_AVERAGE_AVAIL _COUNT	GAUGE	False	The average availability of type ILBC DSP pad during an interval time	True
EVRCB0_PEAK_USED _COUNT	GAUGE	False	The peak usage of type EVRCB0 DSP pad during an interval time	True
EVRCB0_AVERAGE_U SED_COUNT	GAUGE	False	The average usage of type EVRCB0 DSP pad during an interval time	True
EVRCB0_AVERAGE_A VAIL_COUNT	GAUGE	False	The average availability of type EVRCB0 DSP pad during an interval time	True
GSM_PEAK_USED_CO UNT	GAUGE	False	The peak usage of type AMRNB DSP pad during an interval time	True
GSM_AVERAGE_USED _COUNT	GAUGE	False	The average usage of type AMRNB DSP pad during an interval time	True
GSM_AVERAGE_AVAIL _COUNT	GAUGE	False	The average availability of type AMRNB DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
AMRWB_PEAK_USED_COUNT	GAUGE	False	The peak usage of type Amrwb DSP pad during an interval time	True
AMRWB_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type Amrwb DSP pad during an interval time	True
AMRWB_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type Amrwb DSP pad during an interval time	True
G722_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G722 DSP pad during an interval time	True
G722_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G722 DSP pad during an interval time	True
G722_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G722 DSP pad during an interval time	True
TONE_PEAK_USED_COUNT	GAUGE	False	The peak usage of type TONE DSP pad during an interval time	True
TONE_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type TONE DSP pad during an interval time	True
TONE_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type TONE DSP pad during an interval time	True
EVRC_PEAK_USED_COUNT	GAUGE	False	The peak usage of type EVRCB0 DSP pad during an interval time	True
EVRC_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type EVRC DSP pad during an interval time	True
EVRC_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type EVRC DSP pad during an interval time	True
G7221_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G7221 DSP pad during an interval time	True
G7221_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G7221 DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
G7221_AVERAGE_AVAILABLE_COUNT	GAUGE	False	The average availability of type G7221 DSP pad during an interval time	True
EFR_PEAK_USED_COUNT	GAUGE	False	The peak usage of type Efr DSP pad during an interval time	True
EFR_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type Efr DSP pad during an interval time	True
EFR_AVERAGE_AVAILABLE_COUNT	GAUGE	False	The average availability of type Efr DSP pad during an interval time	True
G711SS_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G711Ss DSP pad during an interval time	True
G711SS_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G711Ss DSP pad during an interval time	True
G711SS_AVERAGE_AVAILABLE_COUNT	GAUGE	False	The average availability of type G711Ss DSP pad during an interval time	True
G729V8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G729 V8 DSP pad during an interval time	True
G729V8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G729 V8 DSP pad during an interval time	True
G729V8_AVERAGE_AVAILABLE_COUNT	GAUGE	False	The average availability of type G729 V8 DSP pad during an interval time	True
G726V8_PEAK_USED_COUNT	GAUGE	False	The interval number of Peak usage of type G726 V8 DSP pad during an interval time	True
G726V8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G726 V8 DSP pad during an interval time	True
G726V8_AVERAGE_AVAILABLE_COUNT	GAUGE	False	The average availability of type G726 V8 DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
G711V8_PACKET_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G711Packet V8 DSP pad during an interval time	True
G711V8_PACKET_AVG_USED_COUNT	GAUGE	False	The average usage of type G711Packet V8 DSP pad during an interval time	True
G711V8_PACKET_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type G711Packet V8 DSP pad during an interval time	True
G711SSV8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G711SSPacket V8 DSP pad during an interval time	True
G711SSV8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G711SSPacket V8 DSP pad during an interval time	True
G711SSV8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G711SSPacket V8 DSP pad during an interval time	True
G723V8_PEAK_USED_COUNT	GAUGE	False	The interval number of Peak usage of type G723 V8 DSP pad during an interval time	True
G723V8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G723 V8 DSP pad during an interval time	True
G723V8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G723 V8 DSP pad during an interval time	True
ILBCV8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type ILBC V8 DSP pad during an interval time	True
ILBCV8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type ILBC V8 DSP pad during an interval time	True
ILBCV8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type ILBC V8 DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
G722V8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G722 V8 DSP pad during an interval time	True
G722V8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G722 V8 DSP pad during an interval time	True
G722V8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G722 V8 DSP pad during an interval time	True
G7221V8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type G7221 V8 DSP pad during an interval time	True
G7221V8_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type G7221 V8 DSP pad during an interval time	True
G7221V8_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type G7221 V8 DSP pad during an interval time	True
OPUS_PEAK_USED_COUNT	GAUGE	False	The peak usage of type OPUS DSP pad during an interval time	True
OPUS_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type OPUS DSP pad during an interval time	True
OPUS_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type OPUS DSP pad during an interval time	True
EVS_PEAK_USED_COUNT	GAUGE	False	The peak usage of type EVS DSP pad during an interval time	True
EVS_AVG_USED_COUNT	GAUGE	False	The average usage of type EVS DSP pad during an interval time	True
EVS_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type EVS DSP pad during an interval time	True
SILK8_PEAK_USED_COUNT	GAUGE	False	The peak usage of type SILK8 DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
SILK8_AVG_USED_COUNT	GAUGE	False	The average usage of type SILK8 DSP pad during an interval time	True
SILK8_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type SILK8 DSP pad during an interval time	True
SILK16_PEAK_USED_COUNT	GAUGE	False	The peak usage of type SILK16 DSP pad during an interval time	True
SILK16_AVG_USED_COUNT	GAUGE	False	The average usage of type SILK16 DSP pad during an interval time	True
SILK16_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type SILK16 DSP pad during an interval time	True
AMRWT140_PEAK_USED_COUNT	GAUGE	False	The peak usage of type AMR with T140 DSP pad during an interval time	True
AMRWT140_AVG_USED_COUNT	GAUGE	False	The average usage of type AMR with T140 DSP pad during an interval time	True
AMRWT140_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type AMR with T140 DSP pad during an interval time	True
AMRWBT140_PEAK_USED_COUNT	GAUGE	False	The peak usage of type AMR-WB with T140 DSP pad during an interval time	True
AMRWBT140_AVG_USED_COUNT	GAUGE	False	The average usage of type AMR-WB with T140 DSP pad during an interval time	True
AMRWBT140_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type AMR-WB with T140 DSP pad during an interval time	True

Column Name	Type	Index	Description	canAggregate
G711_WITHOUT_XCODE_RES_PEAK_COUNT	GAUGE	False	The peak count (during the interval time) of G711 legs (terminations) that did not require a DSP resource The processing for the G.711 leg is done by the DSP resource allocated for the other leg in the call.	True
G711_WITHOUT_XCODE_RES_AVG_COUNT	GAUGE	False	The average count (during the interval time) of G.711 legs (terminations) that did not require a DSP resource The processing for the G.711 leg is done by the DSP resource allocated for the other leg in the call.	True
EVS_T140_PEAK_USAGE_COUNT	GAUGE	False	The peak usage of type EVS with T.140 DSP pad during an interval time	False
EVS_T140_AVERAGE_USAGE_COUNT	GAUGE	False	The average usage of type EVS with T.140 DSP pad during an interval time	False
EVS_T140_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type EVS with T.140 DSP pad during an interval time	False
CE_NAME	STRING	False	The name of the compute element for this entry	False

EthernetPortMgmtStats

Column Name	Type	Index	Description	canAggregate
PORT_NAME	STRING	True	The name of this port	False
RX_PACKETS	COUNTER64	False	The number of received packets	True
TX_PACKETS	COUNTER64	False	The number of transmitted packets	True

Column Name	Type	Index	Description	canAggregate
RX_ERRORS	COUNTER	False	The number of bad packets received	True
TX_ERRORS	COUNTER	False	The number of packet transmit failures	True
RX_DROPPED	COUNTER	False	The number of packets dropped due to no receive buffers	True
TX_DROPPED	COUNTER	False	The number of packets dropped due to no transmit buffers	True
CE_NAME	STRING	False	The name of the compute element for this entry	False

EthernetPortPacketStats

Column Name	Type	Index	Description	canAggregate
PORT_NAME	STRING	True	The name of this port	False
RX_PACKETS	COUNTER 64	False	The number of received packets	True
TX_PACKETS	COUNTER 64	False	The number of transmitted packets	True
RX_ERRORS	COUNTER	False	The number of bad packets received	True
TX_ERRORS	COUNTER	False	The number of packet transmit failures	True
RX_DROPPED	COUNTER	False	The number of packets dropped due to no receive buffers	True
TX_DROPPED	COUNTER	False	The number of packets dropped due to no transmit buffers	True
RX_BYTES	COUNTER 64	False	The number of received bytes	True
TX_BYTES	COUNTER 64	False	The number of transmitted bytes	True

Column Name	Type	Index	Description	canAggregate
CE_NAME	STRING	False	The name of the compute element for this entry	False

IcmpGeneralGroupStats

Column Name	Type	Index	Description	canAggregate
CE_NAME	STRING	True	The name of the compute element for this entry	False
IN_MSGS	COUNTER	False	The total number of ICMP messages that the entity received. This counter includes all those counted by icmpInErrors	True
IN_ECHOS	COUNTER	False	The number of ICMP Echo (request) messages received	True
IN_ECHO_REPS	COUNTER	False	The number of ICMP Echo Reply messages received	True
IN_DEST_UNREACHS	COUNTER	False	The number of ICMP Destination Unreachable messages received	True
IN_ERRORS	COUNTER	False	The number of ICMP messages that the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and such)	True
OUT_MSGS	COUNTER	False	The total number of ICMP messages that this entity attempted to send. This counter includes all those counted by icmpOutErrors	True
OUT_ERRORS	COUNTER	False	The number of ICMP messages that this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. Some implementations may not have the types of error that contribute to this counter's value	True
OUT_ECHOS	COUNTER	False	The number of ICMP Echo (request) messages sent	True

Column Name	Type	Index	Description	canAggregate
OUT_ECHO_REP S	COUNTER	False	The number of ICMP Echo Reply messages sent	True
OUT_DEST_UNR EACHS	COUNTER	False	The number of ICMP Destination Unreachable messages sent	True

IpAcOverallStats

Column Name	Type	Index	Description	canAggregate
ACNAME	STRING	True	The name of the address context	False
NAME	IMPLIEDSTRING	True	The name of the address context	False
MATCHED_NO_RU LE	COUNTER	False	The number of times no rule matches	True
CE_NAME	STRING	False	The name of the compute element for this entry	False

IpAcOverallStats_AG

Column Name	Type	Index	Description	canAggregate
ACNAME	STRING	True	The name of the address context	False
NAME	IMPLIEDSTRING	True	The name of the address context	False
MATCHED_NO_RU LE	COUNTER	False	The number of times no rule matches	True
CE_NAME	STRING	False	The name of the compute element for this entry	False

IpAclRuleStats

Column Name	Type	Index	Description	canAggregate
ACNAME	STRING	True	The name of the address context	False
NAME	STRING	True	The name of this IP access control list rule	False
MATCHES	COUNTER	False	The number of times this rule matches	True
POLICER_DISCARDS	COUNTER	False	The number of times the policer for this rule discarded packets	True
CE_NAME	STRING	False	The name of the compute element for this entry	False

IpAclRuleStats_AG

Column Name	Type	Index	Description	canAggregate
ACNAME	STRING	True	The name of the address context	False
NAME	STRING	True	The name of this IP access control list rule	False
MATCHES	COUNTER	False	The number of times this rule matches	True
POLICER_DISCARDS	COUNTER	False	The number of times the policer for this rule discarded packets	True
CE_NAME	STRING	False	The name of the compute element for this entry	False

IpGeneralGroupStats

Column Name	Type	Index	Description	canAggregate
CE_NAME	STRING	True	The name of the compute element for this entry	False

Column Name	Type	Index	Description	canAggregate
IN_RECEIVES	COUNTER	False	The total number of input datagrams received from interfaces, which includes those received in error	True
IN_HDR_ERRORS	COUNTER	False	The number of input datagrams discarded due to errors in their IP headers, which includes bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and such	True
IN_ADDR_ERRORS	COUNTER	False	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address for this entity to receive. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities that are not IP routers and do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address	True
IN_UNKNOWN_PROTOCOLS	COUNTER	False	The number of locally-addressed datagrams successfully received but discarded because of an unknown or unsupported protocol	True
IN_DISCARDS	COUNTER	False	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which the Ribbon Application Management Platform (RAMP) discards (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting re-assembly	True
IN_DELIVERS	COUNTER	False	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP)	True
OUT_REQUESTS	COUNTER	False	The total number of IP datagrams that local IP user- protocols (including ICMP) supplied to IP in requests for transmission. This counter does not include any datagrams counted in ipForwDatagrams	True

Column Name	Type	Index	Description	canAggregate
OUT_DISCARDS	COUNTER	False	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). This counter includes datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.	True
OUT_NO_ROUTE S	COUNTER	False	The number of IP datagrams discarded because no route is found to transmit them to their destination. This counter includes any packets counted in ipForwDatagrams that meet this no-route criterion, which includes any datagrams that a host cannot route because all of its default routers are down.	True
REASM_TIMEOU T	INTEGER	False	The maximum number of seconds that received fragments are held while they await reassembly at this entity	True
REASM_REQDS	COUNTER	False	The number of IP fragments received that need to reassemble at this entity	True
REASM_OKS	COUNTER	False	The number of IP datagrams successfully re-assembled	True
REASM_FAILS	COUNTER	False	The number of failures detected by the IP re-assembly algorithm (timed out, errors, and such). This is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received	True
FRAG_OKS	COUNTER	False	The number of IP datagrams that successfully fragmented at this entity	True
FRAG_FAILS	COUNTER	False	The number of IP datagrams that discard because they need to fragment at this entity but could not, for example, because their Don't Fragment flag was set	True

IpPolicingSystemIntStats

Column Name	Type	Index	Description	canAggregate
SYSTEM_NAME	STRING	True	Name of the system	False
BAD_HDR_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the bad Ethernet/IP Header policer	True
BAD_HDR_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the bad Ethernet/IP Header policer	True
BAD_HDR_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the bad Ethernet/IP Header policer	True
BAD_HDR_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the bad Ethernet/IP Header policer	True
BAD_HDR_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the bad Ethernet/IP Header policer	True
BAD_HDR_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the bad Ethernet/IP Header policer	True
ARP_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the ARP policer	True
ARP_ACCEPT_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the ARP policer	True
ARP_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the ARP policer	True
ARP_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the ARP policer	True
ARP_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the ARP policer	True

Column Name	Type	Index	Description	canAggregate
ARP_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the ARP policer	True
ARP_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the ARP policer	True
UFLOW_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the micro flow policer	True
UFLOW_ACCEPT_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the micro flow policer	True
UFLOW_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the micro flow policer	True
UFLOW_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the micro flow policer	True
UFLOW_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the micro flow policer	True
UFLOW_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the micro flow policer	True
UFLOW_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the micro flow policer	True
ACL_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the access control list policer	True
ACL_ACCEPT_PACKET_COUNT	COUNTER64	False	The current number of accepted packets for the access control list policer	True
ACL_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the access control list policer	True
ACL_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the access control list policer	True

Column Name	Type	Index	Description	canAggregate
ACL_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the access control list policer	True
ACL_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the access control list policer	True
ACL_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the access control list policer	True
AGGREGATE_DISCARD_PKT_COUNT	COUNTER64	False	The current number of discarded packets for the aggregate policer	True
AGGREGATE_ACCEPT_PKT_COUNT	COUNTER64	False	The current number of accepted packets for the aggregate policer	True
AGGREGATE_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the aggregate policer	True
AGGREGATE_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the aggregate policer	True
AGGREGATE_MINOR_ALARM_DUR	GAUGE	False	The current duration of the minor alarms in seconds for the aggregate policer	True
AGGREGATE_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the aggregate policer	True
AGGREGATE_MAJOR_ALARM_DUR	GAUGE	False	The current duration of the major alarms in seconds for the aggregate policer	True
IP_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the IPSEC Decrypt policer	True
IP_ACCEPT_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the IPSEC Decrypt policer	True

Column Name	Type	Index	Description	canAggregate
IP_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the IPSEC Decrypt policer	True
IP_MINOR_ALARM_COUNT	COUNTER	False	The current number of minor alarms for the IPSEC Decrypt policer	True
IP_MINOR_ALARM_DURATION	COUNTER	False	The current duration of the minor alarms in seconds for the IPSEC Decrypt policer	True
IP_MAJOR_ALARM_COUNT	COUNTER	False	The current number of major alarms for the IPSEC Decrypt policer	True
IP_MAJOR_ALARM_DURATION	COUNTER	False	The current duration of the major alarms in seconds for the IPSEC Decrypt policer	True
MEDIA_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the media policer	True
MEDIA_ACCEPT_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the media policer	True
MEDIA_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the media policer	True
MEDIA_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the media policer	True
MEDIA_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the media policer	True
MEDIA_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the media policer	True
MEDIA_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the media policer	True

Column Name	Type	Index	Description	canAggregate
ROGUE_MEDIA_DISCARD_PKT_COUNT	COUNTER64	False	The current number of discarded packets for the rogue media policer	True
ROGUE_MEDIA_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the rogue media policer	True
ROGUE_MEDIA_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the rogue media policer	True
ROGUE_MEDIA_MINOR_ALARM_DUR	GAUGE	False	The current duration of the minor alarms in seconds for the rogue media policer	True
ROGUE_MEDIA_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the rogue media policer	True
ROGUE_MEDIA_MAJOR_ALARM_DUR	GAUGE	False	The current duration of the major alarms in seconds for the rogue media policer	True
DISCARD_RULE_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the IPSEC Decrypt policer	True
DISCARD_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the discard rule	True
DISCARD_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the discard rule	True
DISCARD_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the discard rule	True
DISCARD_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the discard rule	True
DISCARD_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the discard rule	True

Column Name	Type	Index	Description	canAggregate
DECRYPT_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of packets discarded by SRTP decrypt discards	True
PEAK_DECRYPT_DISCARD_RATE	GAUGE	False	The current peak discard rate for SRTP decrypt discards	True
MINOR_DECRYPT_ALARM_COUNT	INTEGER	False	The current number of minor alarms for SRTP decrypt discards	True
MINOR_DECRYPT_ALARM_DURATION	INTEGER	False	The current duration of the minor alarms in seconds for SRTP decrypt discards	True
MAJOR_DECRYPT_ALARM_COUNT	INTEGER	False	The current number of major alarms for the SRTP decrypt discards	True
MAJOR_DECRYPT_ALARM_DURATION	INTEGER	False	The current duration of the major alarms in seconds for SRTP decrypt discards	True
CE_NAME	STRING	False	The name of the compute element for this entry	False

IpPolicingSystemIntStats_AG

Column Name	Type	Index	Description	canAggregate
SYSTEM_NAME	STRING	True	Name of the system	False
BAD_HDR_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the bad Ethernet/IP Header policer	True
BAD_HDR_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the bad Ethernet/IP Header policer	True
BAD_HDR_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the bad Ethernet/IP Header policer	True

Column Name	Type	Index	Description	canAggregate
BAD_HDR_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the bad Ethernet/IP Header policer	True
BAD_HDR_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the bad Ethernet/IP Header policer	True
BAD_HDR_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the bad Ethernet/IP Header policer	True
ARP_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the ARP policer	True
ARP_ACCEPT_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the ARP policer	True
ARP_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the ARP policer	True
ARP_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the ARP policer	True
ARP_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the ARP policer	True
ARP_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the ARP policer	True
ARP_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the ARP policer	True
UFLOW_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the micro flow policer	True
UFLOW_ACCEPT_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the micro flow policer	True

Column Name	Type	Index	Description	canAggregate
UFLOW_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the micro flow policer	True
UFLOW_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the micro flow policer	True
UFLOW_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the micro flow policer	True
UFLOW_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the micro flow policer	True
UFLOW_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the micro flow policer	True
ACL_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the access control list policer	True
ACL_ACCEPT_PACKET_COUNT	COUNTER64	False	The current number of accepted packets for the access control list policer	True
ACL_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the access control list policer	True
ACL_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the access control list policer	True
ACL_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the access control list policer	True
ACL_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the access control list policer	True
ACL_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the access control list policer	True

Column Name	Type	Index	Description	canAggregate
AGGREGATE_DISCARD_PKT_COUNT	COUNTER64	False	The current number of discarded packets for the aggregate policer	True
AGGREGATE_ACCEPT_PKT_COUNT	COUNTER64	False	The current number of accepted packets for the aggregate policer	True
AGGREGATE_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the aggregate policer	True
AGGREGATE_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the aggregate policer	True
AGGREGATE_MINOR_ALARM_DUR	GAUGE	False	The current duration of the minor alarms in seconds for the aggregate policer	True
AGGREGATE_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the aggregate policer	True
AGGREGATE_MAJOR_ALARM_DUR	GAUGE	False	The current duration of the major alarms in seconds for the aggregate policer	True
IP_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the IPSEC Decrypt policer	True
IP_ACCEPT_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the IPSEC Decrypt policer	True
IP_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the IPSEC Decrypt policer	True
IP_MINOR_ALARM_COUNT	COUNTER	False	The current number of minor alarms for the IPSEC Decrypt policer	True
IP_MINOR_ALARM_DURATION	COUNTER	False	The current duration of the minor alarms in seconds for the IPSEC Decrypt policer	True

Column Name	Type	Index	Description	canAggregate
IP_MAJOR_ALARM_COUNT	COUNTER	False	The current number of major alarms for the IPSEC Decrypt policer	True
IP_MAJOR_ALARM_DURATION	COUNTER	False	The current duration of the major alarms in seconds for the IPSEC Decrypt policer	True
MEDIA_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the media policer	True
MEDIA_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the media policer	True
MEDIA_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the media policer	True
MEDIA_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the media policer	True
MEDIA_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the media policer	True
MEDIA_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the media policer	True
ROGUE_MEDIA_DISCARD_PKT_COUNT	COUNTER64	False	The current number of discarded packets for the rogue media policer	True
ROGUE_MEDIA_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the rogue media policer	True
ROGUE_MEDIA_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the rogue media policer	True
ROGUE_MEDIA_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the rogue media policer	True

Column Name	Type	Index	Description	canAggregate
ROGUE_MEDIA_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the rogue media policer	True
ROGUE_MEDIA_MAJOR_ALARM_DUR	GAUGE	False	The current duration of the major alarms in seconds for the rogue media policer	True
DISCARD_RULE_PACKET_COUNT	COUNTER64	False	The current number of discarded packets for the IPSEC Decrypt policer	True
DISCARD_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the discard rule	True
DISCARD_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the discard rule	True
DISCARD_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the discard rule	True
DISCARD_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the discard rule	True
DISCARD_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the discard rule	True
DECRYPT_DISCARD_PACKET_COUNT	COUNTER64	False	The current number of packets discarded by SRTP decrypt discards	True
PEAK_DECRYPT_DISCARD_RATE	GAUGE	False	The current peak discard rate for SRTP decrypt discards	True
MINOR_DECRYPT_ALARM_COUNT	INTEGER	False	The current number of minor alarms for SRTP decrypt discards	True
MINOR_DECRYPT_ALARM_DURATION	INTEGER	False	The current duration of the minor alarms in seconds for SRTP decrypt discards	True

Column Name	Type	Index	Description	canAggregate
MAJOR_DECRYPT_ALARM_COUNT	INTEGER	False	The current number of major alarms for the SRTP decrypt discards	True
MAJOR_DECRYPT_ALARM_DURATION	INTEGER	False	The current duration of the major alarms in seconds for SRTP decrypt discards	True
CE_NAME	STRING	False	The name of the compute element for this entry	False

LinkDetectionGroupStats

Column Name	Type	Index	Description	canAggregate
ACNAME	STRING	True	The name of the address context	False
NAME	STRING	True	The name of this link detection group	False
SINGLE_FAILURES	INTEGER	False	The number of single failures for this link detection group	True
DOUBLE_FAILURES	INTEGER	False	The number of double failures for this link detection group	True
FAILURES	INTEGER	False	The number of >2 failures for this link detection group	True
CE_NAME	STRING	False	The name of the compute element for this entry	False

LinkMonitorStats

Column Name	Type	Index	Description	canAggregate
ACNAME	STRING	True	The name of the address context	False
GNAME	STRING	True	The name of the address context group	False
NAME	STRING	True	The name of the link monitor	False

Column Name	Type	Index	Description	canAggregate
MIN_TIME	INTEGER	False	The minimum time used to get a reply for an echo request packet	True
MAX_TIME	INTEGER	False	The maximum time used to get a reply for an echo request packet	True
AVERAGE_TIME	INTEGER	False	The average time used to get a reply for an echo request packet	True
SINGLE_FAILURES	INTEGER	False	The number of single failures for this IP interface	True
DOUBLE_FAILURES	INTEGER	False	The number of double failures for this IP interface	True
FAILURES	INTEGER	False	The number of >2 failures for this IP interface	True
REPLIES	INTEGER	False	The number of replies	True
DUPLICATE_REPLIES	INTEGER	False	The number of duplicate replies	True
LATE_REPLIES	INTEGER	False	The number of late replies	True
CE_NAME	STRING	False	The name of the compute element for this entry	False

MRFPVmgGeneralIntStats

Column Name	Type	Index	Description	canAggregate
VMG_NAME	STRING	True	The name of this Virtual Media Gateway.	False
TX_REQUESTS_RECEIVED	COUNTER	False	The number of transaction requests received from MGC.	True
TX_RESPONSES_SENT	COUNTER	False	The number of transaction responses sent to MGC.	True
TX_REQUESTS_SENT	COUNTER	False	The number of transaction requests sent to MGC.	True

Column Name	Type	Index	Description	canAggregate
TX_RESPONSES_RECEIVED	COUNTER	False	The number of transaction responses received from MGC.	True
ERRORS_DETECTED	COUNTER64	False	The total number of errors detected.	True
TRANS_LOSSES_DETECTED	COUNTER64	False	The total number of transport losses detected.	True
ADD_REQUESTS	COUNTER	False	The total number of ADD requests received.	True
ADD_RESPONSES	COUNTER	False	The total number of ADD responses sent.	True
AUDIT_VAL_REQUESTS	COUNTER	False	The total number of AUDIT VALUE requests received.	True
AUDIT_VAL_RESPONSES	COUNTER	False	The total number of AUDIT VALUE responses sent.	True
MODIFY_REQUESTS	COUNTER	False	The total number of MODIFY requests received.	True
MODIFY_RESPONSES	COUNTER	False	The total number of MODIFY responses sent.	True
SUBTRACT_REQUESTS	COUNTER	False	The total number of SUBTRACT requests received.	True
SUBTRACT_RESPONSES	COUNTER	False	The total number of SUBTRACT responses sent.	True
NOTIFY_REQUESTS	COUNTER	False	The total number of NOTIFY requests sent.	True
NOTIFY_RESPONSES	COUNTER	False	The total number of NOTIFY responses received.	True
SVC_CHANGE_REQUESTS	COUNTER	False	The total number of SERVICECHANGE requests sent and received.	True

Column Name	Type	Index	Description	canAggregate
SVC_CHANGE_RESPONSES	COUNTER	False	The total number of SERVICECHANGE responses sent and received.	True
INAC_NOTIFY_REQUESTS	COUNTER	False	The number of NOTIFY requests sent with an inactivity event (it/ito).	True
INAC_NOTIFY_RESPONSES	COUNTER	False	The number of NOTIFY responses received with an inactivity event (it/ito).	True
SRESART_SERVICECHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=restart) requests sent.	True
SDISC_SERVICECHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=disconnect) requests sent.	True
SGRACE_SERVICECHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=graceful) requests sent.	True
SFORCE_SERVICECHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=force) requests sent.	True
SHAND_SERVICECHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=handoff) requests sent.	True
SFAIL_SERVICECHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=failover) requests sent.	True
URESART_SERVICECHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=restart) requests sent.	True

Column Name	Type	Index	Description	canAggregate
UDISC_SVC_CHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=disconnect) requests sent.	True
UGRACE_SVC_CHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=graceful) requests sent.	True
UFORCE_SVC_CHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=force) requests sent.	True
UHAND_SVC_CHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=handoff) requests sent.	True
UFAIL_SVC_CHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=failover) requests sent.	True
ADD_NO_TERM_RESP	COUNTER	False	The total number of unsuccessful ADD/MODIFY (cause=NoterminationAvailable) replies sent.	True
ADD_NO_CTX_RESP	COUNTER	False	The total number of unsuccessful ADD (cause=NoContextAvailable) replies sent.	True
INSUFF_RES_RESP	COUNTER	False	The total number of unsuccessful ADD/MODIFY (cause=InsufficientResources) replies sent.	True
SEND_TONE_FAIL_RESP	COUNTER	False	The total number of unsuccessful ADD/MODIFY (cause=ToneFailure) replies sent.	True

Column Name	Type	Index	Description	canAggregate
RETRANS_MSGS	COUNTER	False	The total number of retransmitted messages.	True
PENDING_MSGS	COUNTER	False	The total number of transaction pending messages sent.	True
NO_RTP_RCVD	COUNTER	False	The number of terminations where no RTP was received.	True
NUM_TERM_NO_RTP_RCVD_5SEC	COUNTER	False	The number of terminations where RTP was being received, then RTP stopped for 5 seconds.	True
NUM_TERM_RTP_PKT_LOSS_10PCT	COUNTER	False	The number of terminations where packet loss in the incoming RTP stream exceeded 10%.	True
NUM_TERM_RTP_PKT_LOSS_2PCT	COUNTER	False	The number of terminations where packet loss in the incoming RTP stream exceeded 2%.	True
PCT_TERM_NO_RTP_RCVD	COUNTER	False	The percentage of terminations where, no RTP was received.	True
TOTAL_RTP_TERM	COUNTER	False	The total number of terminations on the VMG.	True
RTP_COUNT_DISCREPANCY	COUNTER	False	The RTP Count Discrepancy between NP and DSP.	True
CE_NAME	STRING	No	The name of the compute element for this entity.	False

MRFPVmgGeneralIntStats_AG

Column Name	Type	Index	Description	canAggregate
VMG_NAME	STRING	True	The name of this Virtual Media Gateway.	False

Column Name	Type	Index	Description	canAggregate
TX_REQUESTS_RECEIVED	COUNTER	False	The number of transaction requests received from MGC.	True
TX_RESPONSES_SENT	COUNTER	False	The number of transaction responses sent to MGC.	True
TX_REQUESTS_SENT	COUNTER	False	The number of transaction requests sent to MGC.	True
TX_RESPONSES_RECEIVED	COUNTER	False	The number of transaction responses received from MGC.	True
ERRORS_DETECTED	COUNTER64	False	The total number of errors detected.	True
TRANS_LOSSES_DETECTED	COUNTER64	False	The total number of transport losses detected.	True
ADD_REQUESTS	COUNTER	False	The total number of ADD requests received.	True
ADD_RESPONSES	COUNTER	False	The total number of ADD responses sent.	True
AUDIT_VAL_REQUESTS	COUNTER	False	The total number of AUDIT VALUE requests received.	True
AUDIT_VAL_RESPONSES	COUNTER	False	The total number of AUDIT VALUE responses sent.	True
MODIFY_REQUESTS	COUNTER	False	The total number of MODIFY requests received.	True
MODIFY_RESPONSES	COUNTER	False	The total number of MODIFY responses sent.	True
SUBTRACT_REQUESTS	COUNTER	False	The total number of SUBTRACT requests received.	True
SUBTRACT_RESPONSES	COUNTER	False	The total number of SUBTRACT responses sent.	True
NOTIFY_REQUESTS	COUNTER	False	The total number of NOTIFY requests sent.	True

Column Name	Type	Index	Description	canAggregate
NOTIFY_RESPONSES	COUNTER	False	The total number of NOTIFY responses received.	True
SVC_CHANGE_REQUESTS	COUNTER	False	The total number of SERVICECHANGE requests sent and received.	True
SVC_CHANGE_RESPONSES	COUNTER	False	The total number of SERVICECHANGE responses sent and received.	True
INAC_NOTIFY_REQUESTS	COUNTER	False	The number of NOTIFY requests sent with an inactivity event (it/ito).	True
INAC_NOTIFY_RESPONSES	COUNTER	False	The number of NOTIFY responses received with an inactivity event (it/ito).	True
SRESART_SVC_CHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=restart) requests sent.	True
SDISC_SVC_CHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=disconnect) requests sent.	True
SGRACE_SVC_CHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=graceful) requests sent.	True
SFORCE_SVC_CHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=force) requests sent.	True
SHAND_SVC_CHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=handoff) requests sent.	True
SFAIL_SVC_CHANGE_REQ	COUNTER	False	The total number of successful SERVICECHANGE (cause=failover) requests sent.	True

Column Name	Type	Index	Description	canAggregate
URESART_SVC_CHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=restart) requests sent.	True
UDISC_SVC_CHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=disconnect) requests sent.	True
UGRACE_SVC_CHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=graceful) requests sent.	True
UFORCE_SVC_CHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=force) requests sent.	True
UHAND_SVC_CHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=handoff) requests sent.	True
UFAIL_SVC_CHANGE_REQ	COUNTER	False	The total number of unsuccessful SERVICECHANGE (cause=failover) requests sent.	True
ADD_NO_TERM_RESP	COUNTER	False	The total number of unsuccessful ADD/MODIFY (cause=NotterminationAvailable) replies sent.	True
ADD_NO_CTX_RESP	COUNTER	False	The total number of unsuccessful ADD (cause=NoContextAvailable) replies sent.	True
INSUFF_RES_RESP	COUNTER	False	The total number of unsuccessful ADD/MODIFY (cause=InsufficientResources) replies sent.	True

Column Name	Type	Index	Description	canAggregate
SEND_TONE_FAIL_RESP	COUNTER	False	The total number of unsuccessful ADD/MODIFY (cause=ToneFailure) replies sent.	True
RETRANS_MSGS	COUNTER	False	The total number of retransmitted messages.	True
PENDING_MSGS	COUNTER	False	The total number of transaction pending messages sent.	True
NO_RTP_RCVD	COUNTER	False	The number of terminations where no RTP was received.	True
NUM_TERM_NO_RTP_RCVD_5SEC	COUNTER	False	The number of terminations where RTP was being received, then RTP stopped for 5 seconds.	True
NUM_TERM_RTP_PKT_LOSS_10PCT	COUNTER	False	The number of terminations where packet loss in the incoming RTP stream exceeded 10%.	True
NUM_TERM_RTP_PKT_LOSS_2PCT	COUNTER	False	The number of terminations where packet loss in the incoming RTP stream exceeded 2%.	True
PCT_TERM_NO_RTP_RCVD	COUNTER	False	The percentage of terminations where, no RTP was received.	True
TOTAL_RTP_TERM	COUNTER	False	The total number of terminations on the VMG.	True
RTP_COUNT_DISCREPANCY	COUNTER	False	The RTP Count Discrepancy between NP and DSP.	True
CE_NAME	STRING	No	The name of the compute element for this entity.	False

MRFPVmgIpTermNotifyIntStats

Column Name	Column Type	Index	Description	canAggregate
VMG_NAME	STRING	True	Tracks the name of this Virtual Media Gateway.	True
HANGTERM_REQ	COUNTER	False	Tracks the number of IP Termination Notify Requests sent for Hanging Termination event(hangterm/thb).	True
HANGTERM_RES	COUNTER	False	Tracks the number of IP Termination Notify Responses received for Hanging Termination event(hangterm/thb).	True
HANGTERM_ERR	COUNTER	False	Tracks the number of IP Termination Notify Responses received for Hanging Termination event(hangterm/thb).	True
APPDATA_INACT_REQ	COUNTER	False	Tracks the number of IP Termination Notify Responses received for App Data Inactivity Detection event(adid/ipstop).	True
APPDATA_INACT_RES	COUNTER	False	Tracks the number of IP Termination Notify Responses received for App Data Inactivity Detection event(adid/ipstop).	True

Column Name	Column Type	Index	Description	canAggregate
APPDATA_INACT_ERR This counter is deprecated in 9.1.0.	COUNTER	False	Tracks the number of IP Termination Notify Errors received for App Data Inactivity Detection event(adid/ipstop).	True
CE_NAME	STRING	No	The name of the compute element for this entity.	False

MRFPVmgIpTermNotifyIntStats_AG

Column Name	Column Type	Index	Description	canAggregate
VMG_NAME	STRING	True	Tracks the name of this Virtual Media Gateway.	True
HANGTERM_REQ	COUNTER	False	Tracks the number of IP Termination Notify Requests sent for Hanging Termination event(hangterm/thb).	True
HANGTERM_RES	COUNTER	False	Tracks the number of IP Termination Notify Responses received for Hanging Termination event(hangterm/thb).	True
HANGTERM_ERR	COUNTER	False	Tracks the number of IP Termination Notify Responses received for Hanging Termination event(hangterm/thb).	True
APPDATA_INACT_REQ	COUNTER	False	Tracks the number of IP Termination Notify Responses received for App Data Inactivity Detection event(adid/ipstop).	True
APPDATA_INACT_RES	COUNTER	False	Tracks the number of IP Termination Notify Responses received for App Data Inactivity Detection event(adid/ipstop).	True

Column Name	Column Type	Index	Description	canAggregate
APPDATA_INACT_ERR This statistic is deprecated in 9.1.0.	COUNTER	False	Tracks the number of IP Termination Notify Errors received for App Data Inactivity Detection event(adid/ipstop).	True
CE_NAME	STRING	No	The name of the compute element for this entity.	False

NBS5200CallCountStats

Column Name	Type	Index	Description	canAggregate
KEY	IMPLIEDSTRING	True	Key value for the call	False

Column Name	Type	Index	Description	canAggregate
CALL_ATTEMPTS	COUNTER	False	Number of call attempts on this server	True
CALL_COMPLETIONS	COUNTER	False	Total number of completed call attempts on this server	True
ACTIVE_CALLS	GAUGE	False	Current number of active managed calls on this server	False
STABLE_CALLS	GAUGE	False	Current number of stable managed calls on this server	False
CE_NAME	STRING	False	The name of the compute element for this entry	False

NBS5200CallCountStats_AG

Column Name	Type	Index	Description	canAggregate
KEY	IMPLIEDSTRING	True	Key value for the call	False
CALL_ATTEMPTS	COUNTER	False	Number of call attempts on this server	True
CALL_COMPLETIONS	COUNTER	False	Total number of completed call attempts on this server	True
ACTIVE_CALLS	GAUGE	False	Current number of active managed calls on this server	False
STABLE_CALLS	GAUGE	False	Current number of stable managed calls on this server	False
CE_NAME	STRING	False	The name of the compute element for this entry	False

SBX5KAcIOffListIntStats

Column Name	Type	Index	Description	canAggregate
ROLE	INTEGER	True	Role of the system.	False
SERIAL_INDEX	INTEGER	True	The index of the system.	True

Column Name	Type	Index	Description	canAggregate
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SBX5KAggregateOffIntStats

Column Name	Type	Index	Description	canAggregate
ROLE	INTEGER	True	Role of the system.	False
SERIAL_INDEX	INTEGER	True	The index of the system.	True
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True

Column Name	Type	Index	Description	canAggregate
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SBX5KArpOffListIntStats

Column Name	Type	Index	Description	canAggregate
ROLE	INTEGER	True	Role of the system.	False
SERIAL_INDEX	INTEGER	True	The index of the system.	True
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True

Column Name	Type	Index	Description	canAggregate
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SBX5KBadEtherIpHdrOffIntStats

Column Name	Type	Index	Description	canAggregate
ROLE	INTEGER	True	Role of the system.	False
SERIAL_INDEX	INTEGER	True	The index of the system.	True
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True

Column Name	Type	Index	Description	canAggregate
ETHER_TYPE	COUNTER	False	The first ethertype found in the Ethernet packet.	True
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SBX5KDiscardRuleOffIntStats

Column Name	Column Type	Index	Description	canAggregate
ROLE	INTEGER	True	Role of the system.	False
SERIAL_INDEX	INTEGER	True	The index of the system.	True
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True
SOURCE_IP_ADDRESS	INTEGER	False	The source IP port of the table entry.	True
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True
DEST_IP_PORT	STRING	False	The destination IP address of the table entry.	True
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True

Column Name	Column Type	Index	Description	canAggregate
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SBX5KEthernetPortPacketPortStatus

Column Name	Column Type	Index	Description	canAggregate
AVG_RX_ACTUAL_BW	Gauge	False	Tracks the Average Incoming Bandwidth used during KPI bin interval in bytes/sec.	True
AVG_TX_ACTUAL_BW	Gauge	False	Tracks the Average Outgoing Bandwidth used during KPI bin interval in bytes/sec.	True
PEAK_RX_ACTUAL_BW	Gauge	False	Tracks the Peak Incoming Bandwidth used during KPI bin interval in bytes/sec.	True
PEAK_TX_ACTUAL_BW	Gauge	False	Tracks the Peak Outgoing Bandwidth used during KPI bin interval in bytes/sec.	True
AVG_RX_ACTUAL_BWUTIL	Gauge	False	Tracks the average incoming BW utilization based on total available port BW instead of negotiated BW.	True
PEAK_RX_ACTUAL_BWUTIL	Gauge	False	Tracks the maximum incoming BW utilization during the KPI bin interval expressed as a percentage of the available BW.	True
AVG_TX_ACTUAL_BWUTIL	Gauge	False	Tracks the average outgoing BW utilization during the KPI bin interval based on total available BW instead of negotiated BW.	True
PEAK_TX_ACTUAL_BWUTIL	Gauge	False	Tracks the maximum outgoing BW utilization during the KPI bin interval expressed as a percentage of the available BW.	True
BWALARM_THRESHOLD_EXCEEDED	Gauge	False	Tracks the total number of times the BW alarm threshold was passed in the upward direction during the bin interval	True
BWALARM_CLEARED	Gauge	False	Tracks the total number of times the BW clear alarm threshold was passed in the downward direction during the bin interval.	True
AVG_USAGE_BW	Gauge	False	Tracks the Average Bandwidth Usage during KPI bin interval	True

Column Name	Column Type	Index	Description	canAggregate
PEAK_USAGE_BW	GAUGE	False	Tracks the Peak Bandwidth Usage during KPI bin interval.	True
CE_NAME	STRING	True	The host name of the server.	False
PORT_NAME	STRING	True	The name of this port.	False
NEGOTIATED_SPEED	INTEGER	False	The interface speed. Packet port speed is not negotiable.	True
LINK_STATE	INTEGER	False	The state of the interface.	True
MAX_BANDWIDTH	GAUGE	False	Maximum bandwidth this port can support, bytes/sec.	True
ALLOCATED_BANDWIDTH	GAUGE	False	Bandwidth the active media streams on this port reserve, bytes/sec.	True
RX_BANDWIDTH	GAUGE	False	Actual Rx bandwidth in use on this port, bytes/sec.	True
TX_BANDWIDTH	GAUGE	False	Actual Tx bandwidth in use on this port, bytes/sec.	True
BANDWIDTH_USAGE	GAUGE	False	Percentage of maximum bandwidth allocated on this port.	True
BANDWIDTH_DEVIATION	GAUGE	False	Percentage of deviation of actual bandwidth from the allocated bandwidth.	True
MAC_ADDRESS	STRING	False	The MAC address of the network interface.	False
IF_INDEX	GAUGE	False	The unique ifIndex of this Packet NIF.	True

SBX5KLicenseUsageStats

Column Name	Type	Index	Description	canAggregate
FEATURE_NAME	INTEGER	True	This dummy key adds to non-config scalar element container, even though only one row is allowed in the container. Without the key, tailf treats the container non-dynamic and calls get_elem per leaf instead of calling get_object per row.	False
LICENSE_MODE	STRING	False	Displays the licensing mode of the SBC.	False
ENCRYPT_ENABLED	INTEGER	False	Set based on whether the encrypt license is available at the SBC.	False
SRTP_ENABLED	INTEGER	False	Set based on whether the SRTP license is available at the SBC.	False
VIDEO_ENABLED	INTEGER	False	Set based on whether the video license is available at the SBC.	False
AMRNB_ENABLED	INTEGER	False	Set based on whether the AMRNB license is available at the SBC.	False
AMRWB_ENABLED	INTEGER	False	Set based on whether the AMRWB license is available at the SBC.	False
EVRC_ENABLED	INTEGER	False	Set based on whether the EVRC license is available at the SBC.	False
NICE_ENABLED	INTEGER	False	Set based on whether the NICEREC license is available at the SBC.	False
MRF_ENABLED	INTEGER	False	Set based on whether the MRF license is available at the SBC.	False
SIPREC_ENABLED	INTEGER	False	Set based on whether the SIPREC license is available at the SBC.	False
VDSPRTU_ENABLED	INTEGER	False	Set based on whether the transcode license is available at the SBC.	False
PDCS_ENABLED	INTEGER	False	Set based on whether the PDCS license is available at the SBC.	False

Column Name	Type	Index	Description	canAggregate
LI_ENABLED	INTEGER	False	Set based on whether the LI license is available at the SBC.	True
RTU_ENABLED	INTEGER	False	Set based on whether the SBCRTU license is available at the SBC.	False
DSPG722_ENABLED	INTEGER	False	Set based on whether the DSPG722 license is available at the SBC.	True
GMP4X1_ENABLED	INTEGER	False	Set based on whether the 4X1GMP license is available at the SBC.	True
SIPI_ENABLED	INTEGER	False	Set based on whether the SIPL license is available at the SBC.	True
SIP323_ENABLED	INTEGER	False	Set based on whether the SIP323 license is available at the SBC.	True
GMP1X10_ENABLED	INTEGER	False	Set based on whether the 1X10GMP license is available at the SBC.	True
POLRTU_ENABLED	INTEGER	False	Set based on whether the POLRTU license is available at the SBC.	False
PSXRTU_ENABLED	INTEGER	False	Set based on whether the PSXRTU license is available at the SBC.	False
CAPACITY_ENABLED	INTEGER	False	Set based on whether the Capacity license is available at the SBC.	True
E911_ENABLED	INTEGER	False	Set based on whether the E911 license is available at the SBC.	True
ENUM_ENABLED	INTEGER	False	Set based on whether the ENUM license is available at the SBC.	True
SWINSTANCE_ENABLED	INTEGER	False	Set based on whether the SWe Instance license is available at the SBC.	True
EVS_ENABLED	INTEGER	False	Set based on whether EVS license is available at the SBC.	True
SILK_ENABLED	INTEGER	False	Set based on whether SILK license is available at the SBC.	True

Column Name	Type	Index	Description	canAggregate
LBINSTANCE_ENABLED	INTEGER	False	Set based on whether SLB license is available at the SLB.	True
SLBSESS_ENABLED	INTEGER	False	Set based on whether SLB sessions license is available at the SBC.	True
MEDIA_PROBE_AUTH	INTEGER	False	Set based on whether MEDIA PROBE license is available at the SBC.	True
WEB_SOCKET_AUTH	INTEGER	False	Set based on whether WEB SOCKET license is available at the SBC	False
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SBX5KMediaOffIntStats

Column Name	Type	Index	Description	canAggregate
ROLE	INTEGER	True	Role of the system.	False
SERIAL_INDEX	INTEGER	True	The index of the system.	True
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True

Column Name	Type	Index	Description	canAggregate
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True
ETHER_TYPE	COUNTER	False	The first ethertype found in the Ethernet packet.	True
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True
DISCARD_COUNT	COUNTER	False	Determines if all discards were from a unique source address.	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SBX5KRogueMediaIntStats

Column Name	Type	Index	Description	canAggregate
ROLE	INTEGER	True	Role of the system.	False
SERIAL_INDEX	INTEGER	True	The index of the system.	True
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True

Column Name	Type	Index	Description	canAggregate
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True
ETHER_TYPE	INTEGER	False	The first ethertype found in the Ethernet packet.	True
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True
RING_TYPE	INTEGER	False	The media ring type.	False
SOURCE_UNIQUE	INTEGER	False	Determines if all discards were from a unique source address.	False
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SBX5KSystemDspStatusDspUsageStats

Column Name	Type	Index	Description	canAggregate
SYSTEM_NAME	STRING	True	Name of the system	False
COMPRESSION_TOTAL	INTEGER	False	Total compression resource capacity on this server	False
COMPRESSION_UTILIZATION	INTEGER	False	Percentage utilization of compression resources on this server	False
COMPRESSION_ALLOCATION_FAILURES	INTEGER	False	Percentage of compression resources allocation failures on this server	False
G711_TOTAL	INTEGER	False	Total G.711 resource capacity on this server	False
G711_UTILIZATION	INTEGER	False	Percentage utilization of G711 resources on this server	False
G726_TOTAL	INTEGER	False	Total G.726 resource capacity on this server	False

Column Name	Type	Index	Description	canAggregate
G726_UTILIZATION	INTEGER	False	Percentage utilization of G726 resources on this server	False
G729AB_TOTAL	INTEGER	False	Total G.729A+B resource capacity on this server	False
G729AB_UTILIZATION	INTEGER	False	Percentage utilization of G729A+B resources on this server	False
G7231_TOTAL	INTEGER	False	Total G.7231 resource capacity on this server	False
G7231_UTILIZATION	INTEGER	False	Percentage utilization of G7231 resources on this server	False
ILBC_TOTAL	INTEGER	False	Total iLBC resource capacity on this server	False
ILBC_UTILIZATION	INTEGER	False	Percentage utilization of iLBC resources on this server	False
ILBC_ALLOC_FAILURES	INTEGER	False	Percentage of iLBC resources allocation failures on this server	False
ECM_TOTAL	INTEGER	False	Total T.38 ECM resource capacity on this server	False
ECM_UTILIZATION	INTEGER	False	Percentage utilization of T.38 ECM resources on this server	False
ECM_ALLOC_FAILURES	INTEGER	False	Percentage of T.38 ECM resources allocation failures on this server	False
TONE_TOTAL	INTEGER	False	Total tone resource capacity on this server	False
TONE_UTILIZATION	INTEGER	False	Percentage utilization of tone resources on this server	False

Column Name	Type	Index	Description	canAggregate
TONE_ALLOC_FAILURES	INTEGER	False	Percentage of tone resource allocation failures on this server	False
EVRCB0_TOTAL	INTEGER	False	Total EVRCB0 resource capacity on this server	False
EVRCB0_UTILIZATION	INTEGER	False	Percentage utilization of EVRCB0 resources on this server	False
EVRCB0_ALLOC_FAILURES	INTEGER	False	Percentage of EVRCB0 resources allocation failures on this server	False
AMRNB_TOTAL	INTEGER	False	Total AMR-NB resource capacity on this server	False
AMRNB_UTILIZATION	INTEGER	False	Percentage utilization of AMR-NB resources on this server	False
AMRNB_ALLOC_FAILURES	INTEGER	False	Percentage of AMR-NB resources allocation failures on this server	False
AMRWB_TOTAL	INTEGER	False	Total AMR-WB resource capacity on this server	False
AMRWB_UTILIZATION	INTEGER	False	Percentage utilization of AMR-WB resources on this server	False
AMRWB_ALLOC_FAILURES	INTEGER	False	Percentage of AMR-WB resources allocation failures on this server	False
G722_TOTAL	INTEGER	False	Total G.722 resource capacity on this server	False
G722_UTILIZATION	INTEGER	False	Percentage utilization of G.722 resources on this server	False
G722_ALLOC_FAILURES	INTEGER	False	Percentage of G.722 resources allocation failures on this server	False

Column Name	Type	Index	Description	canAggregate
EVRC0_TOTAL	INTEGER	False	Total EVRC0 resource capacity on this server	False
EVRC0_UTILIZATION	INTEGER	False	Percentage utilization of EVRC0 resources on this server	False
EVRC0_ALLOC_FAILURES	INTEGER	False	Percentage of EVRC0 resources allocation failures on this server	False
COMPRESSION_AVAILABLE	INTEGER	False	Number of compression resources currently unused and available on this server	False
TONE_AVAILABLE	INTEGER	False	Number of tone resources currently unused and available on this server	False
G7221_TOTAL	INTEGER	False	Total G.722.1 resource capacity on this server	False
G7221_UTILIZATION	INTEGER	False	Percentage utilization of G.722.1 resources on this server	False
EFR_TOTAL	INTEGER	False	Total EFR resource capacity on this server	False
EFR_UTILIZATION	INTEGER	False	Percentage utilization of EFR resources on this server	False
G711SS_TOTAL	INTEGER	False	Total G.711SS (silence suppression) resource capacity on this server	False
G711SS_UTILIZATION	INTEGER	False	Percentage utilization of G.711SS (silence suppression) resources on this server	False
SLOT1_RESOURCES_UTILIZED	INTEGER	False	Total compression/tone resources in use on this module slot	False

Column Name	Type	Index	Description	canAggregate
SLOT2_RESOURCES_UTILIZED	INTEGER	False	Total compression/tone resources in use on this module slot	False
SLOT3_RESOURCES_UTILIZED	INTEGER	False	Total compression/tone resources in use on this module slot	False
SLOT4_RESOURCES_UTILIZED	INTEGER	False	Total compression/tone resources in use on this module slot	False
G711V8_TOTAL	INTEGER	False	Total G.711 V8 resource capacity on this server	False
G711V8_UTILIZATION	INTEGER	False	Percentage utilization of G.711 V8 resources on this server	False
G711SSV8_TOTAL	INTEGER	False	Total G.711SS (silence suppression) V8 resource capacity on this server	False
G711SSV8_UTILIZATION	INTEGER	False	Percentage utilization of G.711SS (silence suppression) V8 resources on this server	False
G726V8_TOTAL	INTEGER	False	Total G.726 V8 resource capacity on this server	False
G726V8_UTILIZATION	INTEGER	False	Percentage utilization of G.726 V8 resources on this server	False
G7231V8_TOTAL	INTEGER	False	Total G723.1 V8 resource capacity on this server	False
G7231V8_UTILIZATION	INTEGER	False	Percentage utilization of G.7231 V8 resources on this server	False
G722V8_TOTAL	INTEGER	False	Total G.722 V8 resource capacity on this server	False

Column Name	Type	Index	Description	canAggregate
G722V8_UTILIZATION	INTEGER	False	Percentage utilization of G.722 V8 resources on this server	False
G7221V8_TOTAL	INTEGER	False	Total G.722.1 V8 resource capacity on this server	False
G7221V8_UTILIZATION	INTEGER	False	Percentage utilization of G.722.1 V8 resources on this server	False
G729ABV8_TOTAL	INTEGER	False	Total G.729A+B V8 resource capacity on this server	False
G729ABV8_UTILIZATION	INTEGER	False	Percentage utilization of G729A+B V8 resources on this server	False
ECMV34_TOTAL	INTEGER	False	Total T.38 ECM V.34 resource capacity on this server	False
ECMV34_UTILIZATION	INTEGER	False	Percentage utilization of T.38 ECM V.34 resources on this server	False
ILBCV8_TOTAL	INTEGER	False	Total iLBC V8 resource capacity on this server	False
ILBCV8_UTILIZATION	INTEGER	False	Percentage utilization of iLBC V8 resources on this server	False
OPUS_TOTAL	INTEGER	False	Total OPUS resource capacity on this server	False
OPUS_UTILIZATION	INTEGER	False	Percentage utilization of OPUS resources on this server	False
OPUS_ALLOC_FAILURES	INTEGER	False	Percentage of OPUS resources allocation failures on this server	False
USAGE_EVS_TOTAL	INTEGER	False	Total EVS resource capacity on this server	False

Column Name	Type	Index	Description	canAggregate
USAGE_EVS_UTILIZATION	INTEGER	False	Percentage utilization of EVS resources on this server	False
USAGE_SILK8_TOTAL	INTEGER	False	Total SILK8 resource capacity on this server	False
USAGE_SILK8_UTILIZATION	INTEGER	False	Percentage utilization of SILK8 resources on this server	False
USAGE_SILK16_TOTAL	INTEGER	False	Total SILK16 resource capacity on this server	False
USAGE_SILK16_UTILIZATION	INTEGER	False	Percentage utilization of SILK16 resources on this server	False
USAGE_AMRNBT140_TOTAL	INTEGER	False	Total AMR-NB with T.140 capacity on this server	False
USAGE_AMRNBT140_UTILIZATION	INTEGER	False	Percentage utilization of AMR-NB with T.140 resources on this server	False
USAGE_AMRWBT140_TOTAL	INTEGER	False	Total AMR-WB with T.140 capacity on this server	False
USAGE_AMRWBT140_UTILIZATION	INTEGER	False	Percentage utilization of AMR-WB with T.140 resources on this server	False
COMP_HP_UTILIZATION	INTEGER	False	Percentage utilization of AMR-WB with T.140 resource on this server	False
RESOURCE_HP_UTILIZATION	INTEGER	False	Percentage utilization of tone resources used for high priority calls on this server	False
DSP_EVS_T140_TOTAL	INTEGER	False	Total EVS with T.140 resource capacity on this server	False
DSP_EVS_T140_UTILIZATION	INTEGER	False	Percentage utilization of EVS with T.140 resources on this server	False

Column Name	Type	Index	Description	canAggregate
CE_NAME	STRING	False	The name of the compute element for this entry	False

SysCpuUtilIntStatsSts

Column Name	Type	Index	Description	canAggregate
CE_NAME	STRING	True	This object indicates the configured CE name	False
CPU	GAUGE	True	The cpu number	False
AVERAGE	GAUGE	False	The average cpu percent utilization for this interval	True
HIGH	GAUGE	False	The high cpu percent utilization for this interval	True
LOW	GAUGE	False	The low cpu percent utilization for this interval	True

SysMemoryUtilIntStatsSts

Column Name	Type	Index	Description	canAggregate
CE_NAME	STRING	True	This object indicates the configured CE name	False
AVERAGE	GAUGE	False	The average memory percent utilization for this interval	True
HIGH	GAUGE	False	The high memory percent utilization for this interval	True
LOW	GAUGE	False	The low memory percent utilization for this interval	True
AVERAGE_SWAP	GAUGE	False	The average swap memory percent utilization for this interval	True
HIGH_SWAP	GAUGE	False	The high swap memory percent utilization for this interval	True

Column Name	Type	Index	Description	canAggregate
LOW_SWAP	GAUGE	False	The low swap memory percent utilization for this interval	True

SystemCongestionIntervalStats

Column Name	Type	Index	Description	canAggregate
NAME	INTEGER	True	This dummy key adds to non-config scalar element container, even though only one row is allowed in container. Without the key, tailf treats the container non-dynamic and calls get_elem per leaf instead of calling get_object per row.	False
LEVEL_MC1_COUNT	COUNTER	False	The current number of transitions into MC1	True
LEVEL_MC1_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC1	True
LEVEL_MC2_COUNT	COUNTER	False	The current number of transitions into MC2	True
LEVEL_MC2_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC2	True
LEVEL_MC3_COUNT	COUNTER	False	The current number of transitions into MC3	True
LEVEL_MC3_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC3	True
OVERLOAD_REJECTS	COUNTER	False	The current number of calls rejected due to system congestion	True
AVG_CALL_RATE	GAUGE	False	The current system average call arrival rate	True
PEAK_CALL_RATE	GAUGE	False	The current system peak call arrival rate	True
CALL_ARRIVALS	COUNTER	False	The current number of call arrivals	True

Column Name	Type	Index	Description	canAggregate
EMERGENCY_CALL_ARRIVALS	COUNTER	False	The current number of SIP emergency calls arrived	True
EMERGENCY_CALL_REJECTS	COUNTER	False	The current number of SIP emergency calls rejected	True
SIP_REG_ARRIVALS	COUNTER	False	The current number of SIP registrations arrived	True
SIP_REG_REJECTS	COUNTER	False	The current number of SIP registrations rejected	True
AVG_REG_RATE	GAUGE	False	The current average SIP registration arrival rate	True
PEAK_REG_RATE	GAUGE	False	The current peak SIP registration arrival rate	True
MAX_ACTIVE_CALLS	GAUGE	False	High watermark of the total number of active calls in the current interval for the system level.	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SystemCongestionIntervalStats_AG

Column Name	Type	Index	Description	canAggregate
NAME	INTEGER	True	This dummy key adds to non-config scalar element container, even though only one row is allowed in container. Without the key, tailf treats the container non-dynamic and calls get_elem per leaf instead of calling get_object per row.	False
LEVEL_MC1_COUNT	COUNTER	False	The current number of transitions into MC1	True
LEVEL_MC1_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC1	True

Column Name	Type	Index	Description	canAggregate
LEVEL_MC2_COUNT	COUNTER	False	The current number of transitions into MC2	True
LEVEL_MC2_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC2	True
LEVEL_MC3_COUNT	COUNTER	False	The current number of transitions into MC3	True
LEVEL_MC3_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC3	True
OVERLOAD_REJECTS	COUNTER	False	The current number of calls rejected due to system congestion	True
AVG_CALL_RATE	GAUGE	False	The current system average call arrival rate	True
PEAK_CALL_RATE	GAUGE	False	The current system peak call arrival rate	True
CALL_ARRIVALS	COUNTER	False	The current number of call arrivals	True
EMERGENCY_CALL_ARRIVALS	COUNTER	False	The current number of SIP emergency calls arrived	True
EMERGENCY_CALL_REJECTS	COUNTER	False	The current number of SIP emergency calls rejected	True
SIP_REG_ARRIVALS	COUNTER	False	The current number of SIP registrations arrived	True
SIP_REG_REJECTS	COUNTER	False	The current number of SIP registrations rejected	True
AVG_REG_RATE	GAUGE	False	The current average SIP registration arrival rate	True
PEAK_REG_RATE	GAUGE	False	The current peak SIP registration arrival rate	True
MAX_ACTIVE_CALLS	GAUGE	False	High watermark of the total number of active calls in the current interval for the system level	True

Column Name	Type	Index	Description	canAggregate
CE_NAME	STRING	False	The name of the compute element for this entry	False

SystemLicenseInfoStats

Column Name	Type	Index	Description	canAggregate
FEATURE_NAME	STRING	True	This object indicates the feature name	False
LICENSE_ID	STRING	True	This object indicates the license ID	False
EXPIRATION_DATE	STRING	False	This object indicates the license expiry date for a feature	False
USAGE_LIMIT	INTEGER	False	This object indicates the usage limit of a feature	True
SOURCE	STRING	False	This object indicates where the licenses is located, nodeLocked or domain	False
IN_USE	GAUGE	False	This object indicates the number of licenses used by the application	False
CE_NAME	STRING	False	The name of the compute element for this entry	False

UdpGeneralGroupStats

Column Name	Column Type	Index	Description	canAggregate
CE_NAME	STRING	Yes	The name of the compute element for this entry	False
IN_DATAGRAMS	COUNTER	No	The total number of UDP datagrams delivered to UDP users	True
OUT_DATAGRAMS	COUNTER	No	The total number of UDP datagrams sent from this entity	True

Column Name	Column Type	Index	Description	canAggregate
UNKNOWN_PORTS	COUNTER	No	The total number of received UDP datagrams for which there was no application at the destination port	True
IN_ERRORS	COUNTER	No	The number of received UDP datagrams that this entity cannot deliver for reasons other than the lack of an application at the destination port	True

SBC 5400 and SBC SWe Statistics

In this section:

- [Call Stats](#)
 - [CallCountIntervalStats](#)
 - [CallCountIntervalStats_AG](#)
 - [CallFailIntervalStats](#)
 - [CallFailIntervalStats_AG](#)
 - [CallIntervalStats](#)
 - [CallIntervalStats_AG](#)
 - [DiamNodeRfIntervalStatistics](#)
 - [DnsGroupDnsServerStats](#)
- [DSP Stats](#)
 - [DspResDspCallIntervalStats](#)
 - [DspResDspCallIntervalStats_AG](#)
 - [DspResDspUsageIntervalStats](#)
 - [DspResDspUsageIntervalStats_AG](#)
 - [EthernetPortMgmtStats](#)
 - [EthernetPortPacketStats](#)
 - [H323SigPortStatisticsStats](#)
 - [IcmpGeneralGroupStats](#)
- [Ip Stats](#)
 - [IpAclOverallStats](#)
 - [IpAclOverallStats_AG](#)
 - [IpAclRuleStats](#)
 - [IpAclRuleStats_AG](#)
 - [IpGeneralGroupStats](#)
 - [IpPolicingSystemIntStats](#)
 - [IpPolicingSystemIntStats_AG](#)
- [Link Stats](#)
 - [LinkDetectionGroupStats](#)
 - [LinkMonitorStats](#)
- [NBS Stats](#)
 - [NBS5200CallCountStats](#)
 - [NBS5200CallCountStats_AG](#)

- NBS5200TGStatusStats_AG
- NBS5200TrunkGroupStatusStats
- RelayIntervalStatistics
- SBCORE Stats
 - SBCCOREFacBlockingStats
 - SBCCOREFacTotBlockStats
 - SBCCOREOodMessageIntStats
 - SBCCORESipIPPresIntStat
 - SBCCORESipIPPresIntStats_AG
 - SBCCORESipRegCountDomIntStats
 - SBCCORESipRegCountDomIntStats_AG
 - SBCCORESipTGAggregatedStats
 - SBCCORESipTgCSSRIntStats
 - SBCCORESipTgCSSRIntStats_AG
 - SBCCORESipTGResIntStats
 - SBCCORESipTGResIntStats_AG
 - SBCCORETGAggregatedStats
- SBX5K Stats
 - SBX5KAclOffListIntStats
 - SBX5KAggregateOffIntStats
 - SBX5KArpOffListIntStats
 - SBX5KBadEtherIpHdrOffIntStats
 - SBX5KDiscardRuleOffIntStats
 - SBX5KDtlsSrtpStats
 - SBX5KEthernetPortPacketPortStatus
 - SBX5KIpSecDecryptOffIntStats
 - SBX5KLicenseUsageStats
 - SBX5KMediaOffIntStats
 - SBX5KMtrmConnPortPeerStats
 - SBX5KRogueMediaIntStats
 - SBX5KSipByeResponseIntervalStats
 - SBX5KSipInviteResponseIntervalStats
 - SBX5KSipIpPeerIntervalStats
 - SBX5KSipOptResponseIntervalStats
 - SBX5KSipRegResponseIntervalStats
 - SBX5KSrtpDecryptOffIntStat
 - SBX5KSystemDspStatusDspUsageStats
 - SBX5KUflowOffListIntStats
- Shared CAC Stats
 - SharedCacFailureIntStats
 - SharedCacIntervalStatistics
- SIP Stats
 - SipIntervalStats
 - SipIntervalStats_AG
 - SipIpPeerOptionsIntervalStats
 - SipIpPeerOptionsIntervalStats_AG
 - SipLocalRegistrarRegCountIntStats
 - sipOcsCallIntervalStatistics
 - SipRegCountStats
 - SipRegCountStats_AG
 - SipSigConnStatisticsStats

- SipSigPortStatisticsStats
- SipSigPortStatisticsStats_AG
- SipSigPortTlsStats
- SipSubCountStats
- SipSubCountStats_AG
- SipTrunkGroupOptionsIntervalStats
- SipTrunkGroupOptionsIntervalStats_AG
- Sys Stats
 - SysCongestionIntervalStats_AG
 - SysCpuUtilIntStatsSts
 - SysMemoryUtilIntStatsSts
 - SystemCongestionIntervalStats
 - SystemLicenseInfoStats
 - TcpGeneralGroupStats
 - TrafficControlStats
 - UdpGeneralGroupStats
 - ZoneIntervalStatisticsStats
 - ZoneIntervalStatisticsStats_AG

The statistics tables listed in the page are applicable for the following products:

- SBC 5400
- SBC Software Edition (SWe)

Note

- The statistics tables names are listed in the following format
<name of the table in the exported CSV file>/<name of the table in the Ribbon Application Management Platform (RAMP) PM profile>
- If the table name is same in the exported CSV file and the RAMP PM profile, it is listed only once.

The following columns are listed in the exported CSV files:

- #NODE_ID
The name of the node from which the performance statistics data is collected.

Note

#NODE_ID is available only in stats tables collected at the node level.

#CLUSTER_ID

- The name of the cluster from which the performance statistics data is collected.

Note

#CLUSTER_ID is available only in stats tables aggregated at the cluster level.

- **TIMESTAMP**

The date and time at which the performance statistics data is collected.

Call Stats

CallCountIntervalStats

Column Name	Column Type	Index	Description	canAggregate
NAME	INTEGER	True	This adds a dummy key to non-config scalar element container, even though only one row is allowed in container. Without the key, tailf treats the container non-dynamic and calls get_elem per leaf instead of calling get_object per row.	True
MAX_SESSION_COUNT	COUNTER	False	Displayed as maxSessionCallCount. The high watermark of total number of calls for the specified interval. This statistic accounts for calls that are stable.	True
MAX_POL_RTU_COUNT	INTEGER	False	Displays the same count as MAX_SESSION_COUNT if SBC is using SBC-POL-RTU license. If SBC is not using SBC-POL-RTU license, the count is displayed as 0.	True
ENCRYPT_COUNT	COUNTER	False	Displayed as system wide total encrypt Call Count. The high watermark of total number of encrypt calls for the specified interval.	True
SRTP_COUNT	COUNTER	False	Displayed as system wide total Secure Real-time Transport Protocol (SRTP) Call Count; The high watermark of total number of SRTP calls for the specified interval.	True
VIDEO_COUNT	COUNTER	False	Displayed as system wide total video Call Count; The high watermark of total number of video calls for the specified interval.	True
AMRNB_COUNT	COUNTER	False	The high watermark of total number of Adaptive Multi-Rate Narrowband (AMRNB) calls for the specified interval.	True

Column Name	Column Type	Index	Description	canAggregate
AMRWB_COUNT	COUNTER	False	The high watermark of total number of Adaptive Multi-Rate Wideband (AMRWB) calls for the specified interval.	True
EVRC_COUNT	COUNTER	False	The high watermark of total number of Enhanced Variable Rate Codec (EVRC) calls for the specified interval.	True
NICEREC_COUNT	COUNTER	False	The current high watermark of total number of NICE recording calls.	True
MRFSESS_COUNT	COUNTER	False	The current high watermark of total number of Media Resource Function (MRF) calls.	True
MAX_PSX_RTU_COUNT	INTEGER	False	Displays MAX_SESSION_COUNT when SBC is using SBC-PSX-RTU license. If SBC is not using SBC-PSX-RTU license it displays the count as 0.	True
VDSPRTU_COUNT	COUNTER	False	The high watermark of total number of trans-coded sessions for the specified interval.	True
PDCS_COUNT	COUNTER	False	The high watermark of total number of pdcs header sessions for the specified interval.	True
SIPREC_COUNT	COUNTER	False	The current high watermark of total number of sip recording calls.	True
LI_ENABLED	INTEGER	False	Set based on whether LI license is available at the SBC.	True
DSPG722_ENABLED	INTEGER	False	Set based on whether DspG722 license is available at the SBC.	True
GMP4X1_ENABLED	INTEGER	False	Set based on whether 4X1GMP license is available at the SBC.	True
SIPI_ENABLED	INTEGER	False	Set based on whether Sipl license is available at the SBC.	True

Column Name	Column Type	Index	Description	canAggregate
SIP323_ENABLED	INTEGER	False	Set based on whether SipRec license is available at the SBC.	True
GMP1X10_ENABLED	INTEGER	False	Set based on whether 1X10GMP license is available at the SBC.	True
CAPACITY_ENABLED	INTEGER	False	Set based on whether Capacity license is available at the SBC.	True
E911_ENABLED	INTEGER	False	Set based on whether E911 license is available at the SBC.	True
ENUM_ENABLED	INTEGER	False	Set based on whether ENUM license is available at the SBC.	True
SWINSTANCE_ENABLED	INTEGER	False	Set based on whether Swe Instance license is available at the SBC.	True
EVS_COUNT	COUNT	False	The high watermark of total number of Enhanced Voice Services (EVS) calls for the specified interval.	True
SILK_COUNT	COUNT	False	The high watermark of total number of SILK Codec Transcode calls for the specified interval.	True
SBCRCS_COUNT	COUNT	False	The high watermark of total number of OOD calls that use an RCS based service for the specified interval.	True
HPC_QUE_ATTEMPT	COUNT	False	The number of HPC calls successfully placed on HPC Call Queuing queues for the reporting interval.	True
SLBSESS_COUNT	COUNT	False	Displayed as system wide total stable SLB sessions Count. The high watermark of the total number of active calls for the reporting interval.	True
LBINSTANCE_ENABLED	INTEGER	False	Set based on whether SLB license is available at the SLB.	False

Column Name	Column Type	Index	Description	canAggregate
HPC_QUE_OVERFLOW	COUNT	False	The number of HPC calls which experienced unsuccessful call queuing attempts due to full queues for the reporting interval.	True
HPC_QUE_ABANDON	COUNT	False	The number of queued HPC calls abandoned before call completion during the reporting interval.	True
HPC_QUE_TIMEOUTS	COUNT	False	The number of HPC calls removed from the queue due to expiration of the queue timeout timer for the reporting interval.	True
HPC_CTL_TFC_EXEM	COUNT	False	The HPC traffic control exemptions for this reporting interval.	True
SOSBC_RTU_COUNT	COUNTER	False	The system wide total stable SOSBC sessions count. The high water mark of total number of active calls for the reporting interval.	True
WEB_SOCKET_COUNT	COUNTER	False	The high water mark of total number of web socket calls for this reporting interval.	True
NOTRUF_AUTH	INTEGER	True	Set based on whether NOTRUF license is available at the SBC.	False
CE_NAME	STRING	False	The name of the compute element for this entry.	False
CALL_COUNT_CNE	COUNTER	False	Displayed as system wide total CNE sessions Count. The high water mark of total number of active calls for the reporting interval.	True
L16_LEG_COUNT	COUNTER	False	The high water mark of total number of L16 call legs for the reporting interval.	True
T140	INTEGER	False	Set based on whether the t140 code is used on at least one call leg for the current interval.	True

Column Name	Column Type	Index	Description	canAggregate
DOD	INTEGER	False	Set based on when the application is running in DOD mode.	True
FIPS	INTEGER	False	Set based on when the application is running in FIPS mode.	True
CNEINSTANCE_ENABLED	INTEGER	False	Set based on whether cneInstance license is available at the SBC.	True

CallCountIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
NAME	INTEGER	True	This adds a dummy key to non-config scalar element container, even though only one row is allowed in container. Without the key, tailf treats the container non-dynamic and calls get_elem per leaf instead of calling get_object per row.	false	N/A
SUM_MAX_SESSION_COUNT	COUNTER	False	The sum of the high watermark of total number of calls for the specified interval. This statistic accounts for calls that are stable. Displayed as maxSessionCallCount.	True	SUM
SUM_MAX_POL_RTU_COUNT	INTEGER	False	The sum of the MAX_SESSION_COUNT if SBC is using SBC-POL-RTU license. If SBC is not using SBC-POL-RTU license, the count is displayed as 0.	True	SUM
SUM_ENCRYPT_COUNT	COUNTER	False	The sum of the system wide total encrypt Call Count. The high watermark of total number of encrypt calls for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SRTP_COUNT	COUNTER	False	The sum of the system wide total Secure Real-time Transport Protocol (SRTP) Call Count; The high watermark of total number of SRTP calls for the specified interval.	True	SUM
SUM_VIDEO_COUNT	COUNTER	False	The sum of the system wide total video Call Count; The high watermark of total number of video calls for the specified interval.	True	SUM
SUM_AMRNB_COUNT	COUNTER	False	The sum of the high watermark of total number of Adaptive Multi-Rate Narrowband (AMRNB) calls for the specified interval.	True	SUM
SUM_AMRWB_COUNT	COUNTER	False	The sum of the high watermark of total number of Adaptive Multi-Rate Wideband (AMRWB) calls for the specified interval.	True	SUM
SUM_EVRC_COUNT	COUNTER	False	The sum of the high watermark of total number of Enhanced Variable Rate Codec (EVRC) calls for the specified interval.	True	SUM
SUM_NICEREC_COUNT	COUNTER	False	The sum of the current high watermark of total number of NICE recording calls.	True	SUM
SUM_MRFSESS_COUNT	COUNTER	False	The sum of the current high watermark of total number of Media Resource Function (MRF) calls.	True	SUM
SUM_MAX_PSSX_RTU_COUNT	INTEGER	False	The sum of the MAX_SESSION_COUNT when SBC is using SBC-PSX-RTU license. If SBC is not using SBC-PSX-RTU license it displays the count as 0.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_VDSPRT U_COUNT	COUNTER	False	The sum of the high watermark of total number of trans-coded sessions for the specified interval.	True	SUM
SUM_PDCS_C OUNT	COUNTER	False	The sum of the high watermark of total number of pdcs header sessions for the specified interval.	True	SUM
SUM_SIPREC_ COUNT	COUNTER	False	The sum of the current high watermark of total number of sip recording calls.	True	SUM
SUM_LI_ENAB LED	INTEGER	False	The sum of the count of LI licenses available at the SBC.	True	SUM
SUM_DSPG72 2_ENABLED	INTEGER	False	The sum of the count of DspG722 licenses available at the SBC.	True	SUM
SUM_GMP4X1 _ENABLED	INTEGER	False	The sum of the count of 4X1GMP licenses is available at the SBC.	True	SUM
SUM_SIPI_EN ABLED	INTEGER	False	The sum of the count of Sipl licenses available at the SBC.	True	SUM
SUM_SIP323_ ENABLED	INTEGER	False	The sum of the count of SipRec licenses available at the SBC.	True	SUM
SUM_GMP1X1 0_ENABLED	INTEGER	False	The sum of the count of 1X10GMP licenses available at the SBC.	True	SUM
SUM_CAPACIT Y_ENABLED	INTEGER	False	The sum of the count of Capacity licenses available at the SBC.	True	SUM
SUM_E911_EN ABLED	INTEGER	False	The sum of the count of E911 licenses available at the SBC.	True	SUM
SUM_ENUM_E NABLED	INTEGER	False	The sum of the count of ENUM licenses available at the SBC.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SWINST ANCE_ENABLED	INTEGER	False	The sum of the count of SWe Instance licenses available at the SBC.	True	SUM
SUM_EVS_CO UNT	COUNT	False	The sum of the high watermark of total number of Enhanced Voice Services (EVS) calls for the specified interval.	True	SUM
SUM_SILK_CO UNT	COUNT	False	The sum of the high watermark of total number of SILK Codec Transcode calls for the specified interval.	True	SUM
SUM_SBCRCS _COUNT	COUNT	False	The sum of the high watermark of total number of OOD calls that use an RCS based service for the specified interval.	True	SUM
SUM_LBINSTA NCE_ENABLED	INTEGER	False	The sum of the count of SLB licenses available at the SLB.	True	SUM
SUM_SLB_SES S_COUNT	COUNTER	False	The sum of the total stable SLB sessions count across the system. The high watermark of total number of active calls for the reporting interval.	True	SUM
SUM_HPC_QU E_ATTEMPT	COUNTER	False	The sum of the number of HPC calls that were successfully placed on HPC Call Queuing queues for the reporting interval.	True	SUM
SUM_HPC_QU E_OVERFLOW	COUNTER	False	The sum of the number of HPC calls for which HPC call queuing attempts were unsuccessful because queues were full for the reporting interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_HPC_QUEUE_ABANDON	COUNTER	False	The sum of the number of HPC calls that were placed in HPC Call Queuing queues, but were subsequently abandoned before they are completed for the reporting interval.	True	SUM
SUM_HPC_QUEUE_TIMEOUTS	COUNTER	False	The sum of the number of HPC calls that were placed in HPC Call Queuing queues, but were subsequently abandoned before they are completed for the reporting interval.	True	SUM
SUM_HPC_CTRL_TFC_EXEM	COUNTER	False	The sum of the HPC traffic control exemptions for this reporting interval.	True	SUM
SUM_SOSBC_RTU_COUNT	COUNTER	False	The system wide total stable SOSBC sessions count. The high water mark of total number of active calls for the reporting interval.	True	SUM
AVG_LBINSTANCED_ENABLE	INTEGER	False	Set based on whether the SLB license is available at the SLB.	True	MEAN
AVG_LICENSE_MODE	INTEGER	False	Displays the licensing mode of the SBC.	True	MEAN
WEB_SOCKET_COUNT	COUNTER	False	The high water mark of total number of web socket calls for this reporting interval.	True	SUM
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

CallFailIntervalStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ZNAME	STRING	Yes	The name of the address context zone.	False	
NAME	STRING	Yes	The name of this trunk group.	True	
IN_CALL_FAIL_NO_ROUTES	COUNTER	No	Number of inbound failed calls because there was no route available for this trunk group for the specified interval.	False	
IN_CALL_FAIL_NO_RESOURCES	COUNTER	No	Number of inbound failed calls because there was an unavailable resource for this trunk group for the specified interval.	True	
IN_CALL_FAIL_NO_SERVICE	COUNTER	No	Number of inbound failed calls because there was an unavailable service for this trunk group for the specified interval.	True	
IN_CALL_FAIL_INVALID_CALL	COUNTER	No	Number of inbound failed calls because there was an invalid call attempt for this trunk group for the specified interval.	True	
IN_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	Number of inbound failed calls because there was a network failure for this trunk group for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
IN_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	The number of failed inbound calls due to a protocol error for this trunk group for the specified interval. The SBC increments the counter for this statistic when it receives unrecognized parameters, or all the required parameters are not configured.	True	
IN_CALL_FAIL_UNSPECIFIED	COUNTER	No	Number of inbound failed calls for an unspecified reason for this trunk group for the specified interval.	True	
OUT_CALL_FAIL_NO_ROUTES	COUNTER	No	Number of outbound failed calls due to no route available for this trunk group for the specified interval.	True	
OUT_CALL_FAIL_NO_RESOURCES	COUNTER	No	The number of failed outbound calls due to unavailable resources for this trunk group for the specified interval. The SBC increments the counter for this statistic when the route is not configured and it fails to find the necessary resources.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
OUT_CALL_FAIL_NO_SERVICE	COUNTER	No	The number of failed outbound calls due to service unavailability for this trunk group for the specified interval. The SBC increments the counter for this statistic when outbound call service is not available for this trunk group during the specified interval.	True	
OUT_CALL_FAIL_INVALID_CALL	COUNTER	No	Number of outbound failed calls due to invalid call attempt for this trunk group for the specified interval.	True	
OUT_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	Number of outbound failed calls due to network failure for this trunk group for the specified interval.	True	
OUT_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	The number of failed outbound calls due to a protocol error for this trunk group for the specified interval. The SBC increments the counter for this statistic when it receives unrecognized parameters, or all the required parameters are not configured.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
OUT_CALL_FAIL_UNSPECIFIED	COUNTER	No	The number of failed outbound calls due to an unspecified reason for this trunk group for the specified interval. The SBC increments the counter for this statistic if the SIP Signaling Port for the egress is disabled while calls are in progress.	True	
ROUTING_FAILURES_RESERVED	COUNTER	No	Number of routing failures due to all circuits reserved for this trunk group for specified interval.	True	
ALLOC_FAIL_BW_LIMIT	COUNTER	No	The number of failed bandwidth requests due to the current usage exceeding the configured bandwidth limit for this trunk group for the specified interval.	True	
ALLOC_FAIL_CALL_LIMIT	COUNTER	No	The number of failed call handling requests due to the current number of concurrent calls exceeding the configured call limit for this trunk group for the specified interval.	True	
NO_PBX_ROUTE	COUNTER	No	Number of failed calls on an ingress trunk group due to no routes returned from the ERE for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
CALL_ABANDONED	COUNTER	No	Number of calls on a toll-free TG that were abandoned while dialing for the specified interval.	True	
CALL_FAIL_POLICING	COUNTER	No	The number of calls for a trunk group that failed during the specified interval due to configured policing rules in the SBC.	True	
SIP_REG_FAIL_POLICING	COUNTER	No	Number SIP registration attempts that failed due to policing on TG for specified interval.	True	
SIP_REG_FAIL_INTERNAL	COUNTER	No	Number SIP registration attempts that failed due to other reasons (signaling failures, and so on) on a trunk group for the specified interval.	True	
SIP_REG_FAIL_OTHER	COUNTER	No	The current number SIP registration attempts that failed due to other reasons (signaling failures, and so on) on a trunk group for the specified interval.	True	
SECURITY_FAIL	COUNTER	No	Number of calls that failed due to mismatch between the peer security and route packet service profile security on trunk group for specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
NON_REG_CALLS_FAILED	COUNTER	No	Number of failed calls due to registration requirement for SIP trunk group for the specified interval.	True	
NON_MATCH_SRC_IP_CALLS_FAILED	COUNTER	No	Number of calls that failed due to mismatched source IP of IAD according to its RCB for the specified interval.	True	
INVALID_SIP_CALLS_FAILED	COUNTER	No	Number of failed calls due to mismatched ingress signaling port from CP according to RCB for the specified interval.	True	
SIP_SUBS_FAIL_POLICING	COUNTER	No	Number of SIP Subscribe attempts that failed due to policing on a trunk group.	True	
SIP_OTHER_REQ_FAIL_POLICING	COUNTER	No	Number of SIP other non-invite attempts that failed due to policing on trunk group.	True	
SIP_OTHER_REQ_FAIL_INTERNAL	COUNTER	No	The count of SIP other non-invite attempts that failed due to policing on a trunk group.	True	
SIP_OTHER_REQ_FAIL_OTHER	COUNTER	No	The count of SIP other non-invite attempts that failed due to policing on a trunk group.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
VIDEO_THRESHOLD_LIMIT	COUNTER	No	The count of exceeded video threshold limits for this shared CAC limits pool.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

CallFailIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
ZNAME	STRING	Yes	The name of the address context zone.	False	N/A
NAME	STRING	Yes	The name of this trunk group.	False	N/A
SUM_IN_CALL_FAIL_NO_ROUTES	COUNTER	No	The sum of the number of inbound failed calls because there was no route available for this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_FAIL_NO_RESOURCES	COUNTER	No	The sum of the number of inbound failed calls because there was an unavailable resource for this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_FAIL_NO_SERVICE	COUNTER	No	The sum of the number of inbound failed calls because there was an unavailable service for this trunk group for the specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_IN_CALL_FAIL_INVALID_CALL	COUNTER	No	The sum of the number of inbound failed calls because there was an invalid call attempt for this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	The sum of the number of inbound failed calls because there was a network failure for this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	The sum of the number of inbound failed calls because there was a protocol error for this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_FAIL_UNSPECIFIED	COUNTER	No	The sum of the number of inbound failed calls for an unspecified reason for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_NO_ROUTES	COUNTER	No	The sum of the number of outbound failed calls due to no route available for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_NO_RESOURCES	COUNTER	No	The sum of the number of outbound failed calls due to unavailable resource for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_NO_SERVICE	COUNTER	No	The sum of the number of outbound failed calls due to unavailable service for this trunk group for the specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_OUT_CALL_FAIL_INVALID_CALL	COUNTER	No	The sum of the number of outbound failed calls due to invalid call attempt for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	The sum of the number of outbound failed calls due to network failure for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	The sum of the number of outbound failed calls due to protocol error for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_UNSPECIFIED	COUNTER	No	The sum of the number of outbound failed calls for an unspecified reason for this trunk group for the specified interval.	True	SUM
SUM_ROUTING_FAILURES_RESERVED	COUNTER	No	The sum of the number of routing failures due to all circuits reserved for this trunk group for specified interval.	True	SUM
SUM_ALLOC_FAIL_BW_LIMIT	COUNTER	No	The sum of the number of bandwidth Requests which fail because the specified interval for this trunk group exceeds the configured bandwidth limit.	True	SUM
SUM_ALLOC_FAIL_CALL_LIMIT	COUNTER	No	The sum of the number of bandwidth Requests which fail because the specified interval for this trunk group exceeds the configured call limit.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NO_PSX_ROUTE	COUNTER	No	The sum of the number of failed calls on an ingress trunk group due to no routes returned from the ERE for the specified interval.	True	SUM
SUM_CALL_ABANDONED	COUNTER	No	The sum of the number of calls on a toll-free TG that were abandoned while dialing for the specified interval.	True	SUM
SUM_CALL_FAIL_POLICING	COUNTER	No	The sum of the number of calls on a trunk group that failed due to policing for the specified interval.	True	SUM
SUM_SIP_REG_FAIL_POLICING	COUNTER	No	The sum of the number SIP registration attempts that failed due to policing on TG for specified interval.	True	SUM
SUM_SIP_REG_FAIL_INTERNAL	COUNTER	No	The sum of the number SIP registration attempts that failed due to other reasons (signaling failures, and so on) on a trunk group for the specified interval.	True	SUM
SUM_SIP_REG_FAIL_OTHER	COUNTER	No	The sum of the current number SIP registration attempts that failed due to other reasons (signaling failures, and so on) on a trunk group for the specified interval.	True	SUM
SUM_SECURITY_FAIL	COUNTER	No	The sum of the number of calls that failed due to mismatch between the peer security and route packet service profile security on trunk group for specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NON_REG_CALLS_FAILED	COUNTER	No	The sum of the number of failed calls due to registration requirement for SIP trunk group for the specified interval.	True	SUM
SUM_NON_MATCH_SRC_IP_CALLS_FAIL	COUNTER	No	The sum of the number of calls that failed due to mismatched source IP of IAD according to its RCB for the specified interval.	True	SUM
SUM_INVALID_SP_CALLS_FAILED	COUNTER	No	The sum of the number of failed calls due to mismatched ingress signaling port from CP according to RCB for the specified interval.	True	SUM
SUM_SIP_SUBS_FAIL_POLICING	COUNTER	No	The sum of the number of SIP Subscribe attempts that failed due to policing on a trunk group.	True	SUM
SUM_SIP_OTHER_REQ_FAIL_POLICING	COUNTER	No	The sum of the number of SIP other non-invite attempts that failed due to policing on trunk group.	True	SUM
SUM_SIP_OTHER_REQ_FAIL_INTERNAL	COUNTER	No	The number of SIP other non-invite attempts that failed due to policing on a trunk group.	True	SUM
SUM_SIP_OTHER_REQ_FAIL_OTHER	COUNTER	No	The number of SIP other non-invite attempts that failed due to policing on a trunk group.	True	SUM
SUM_VIDEO_THRESHOLD_LIMIT	COUNTER	No	The number of video threshold limit exceeded for this trunk group for the specified interval.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

CallIntervalStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context zone.	False	
NAME	STRING	Yes	The name of this trunk group.	True	
IN_USAGE	COUNTER	No	The duration, in seconds, for which all inbound calls in a given interval are using the trunkgroup. This metric is derived using the formula: (total # of inbound calls on the TG) * (interval size) * 60	False	
OUT_USAGE	COUNTER	No	The duration, in seconds, for which all outbound calls in a given interval are using the trunkgroup. This metric is derived using the formula: (total # of outbound calls on the TG) * (interval size) * 60.	True	
IN_CALLS	COUNTER	No	Number of completed inbound calls on this trunk group for the specified interval.	True	
OUT_CALLS	COUNTER	No	Number of completed outbound calls on this trunk group for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
IN_CALL_ATTEMPTS	COUNTER	No	Number of inbound call attempts on this trunk group for the specified interval.	True	
OUT_CALL_ATTEMPTS	COUNTER	No	Number of outbound call attempts on this trunk group for the specified interval.	True	
MAX_COMPLETED_CALLS	COUNTER	No	The high watermark of total number of active calls in both the inbound and outbound directions on the trunk group for the specified interval. This statistic accounts for calls that are setting up, stable, or tearing down.	True	
CALL_SETUP_TIME	COUNTER	No	Total call setup time for all completed calls in inbound and outbound directions for this trunk group for specified interval measured in hundredths of a second.	True	
CALL_SETUPS	COUNTER	No	Total number of calls setup but not necessarily completed in the inbound and outbound directions for this trunk group for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROUTING_ATTEMPTS	COUNTER	No	The number of routing attempts for this trunk group for the specified interval. Each PSX dip can return up to 200 routes. The SBC selects routes based on a number of criteria such as CAC and bandwidth availability. In some cases, crankback/ route advance is needed if the first selected route fails. This metric counts the number of routes attempted before the call succeeded. If the first route succeeds, this counter = 1.	True	
IN_BW_USAGE	COUNTER	No	Sum of bandwidth usage (expected data rate in Kbits per second multiplied by call duration in seconds) for every inbound call associated with this trunk group for the specified interval.	True	
OUT_BW_USAGE	COUNTER	No	Sum of bandwidth usage (expected data rate in Kbits per second multiplied by call duration in seconds) in the outbound direction for this trunk group in seconds in the current interval. The trunk group usage is defined as the time a trunk is seized to the time a trunk is released.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
MAX_ACTIVE_BW_USAGE	GAUGE	No	High watermark bandwidth usage (in Kbits per second) in either direction associated with this trunk group for the specified interval.	True	
CALLS_WITH_PKT_OUTAGE	COUNTER	No	Number of calls with a maximum packet outage whose duration exceeds the configured minimum for this trunk group for the specified interval.	True	
CALLS_WITH_PKT_OUTAGE_AT_END	COUNTER	No	Number of calls whose maximum packet outage occurs at the end of the call for this trunk group for the specified interval.	True	
TOTAL_PKT_OUTAGE	COUNTER	No	Summation of packet outage duration (in milliseconds) whose duration exceeds the configured minimum which is reported during the specified performance interval.	True	
MAX_PKT_OUTAGE	GAUGE	No	Single longest maximum reported packet outage duration (in milliseconds) experienced during the specified performance interval for this trunk group.	True	
POD_EVENTS	COUNTER	No	Number of Packet Outage Detection (POD) Events detected for this peer group for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
PLAYOUT_BUFFER_GOOD	COUNTER	No	Number of calls with all sub-intervals reporting GOOD playout buffer quality for this trunk group for the specified interval.	True	
PLAYOUT_BUFFER_ACCEPTABLE	COUNTER	No	Number of calls with all sub-intervals reporting ACCEPTABLE or better playout buffer quality for this trunk group for the specified interval.	True	
PLAYOUT_BUFFER_POOR	COUNTER	No	Number of calls with all sub-intervals reporting POOR or better playout buffer quality for this trunk group for the specified interval.	True	
PLAYOUT_BUFFER_UNACCEPTABLE	COUNTER	No	Number of calls with at least one sub-interval reporting UNACCEPTABLE playout buffer quality for this trunk group for the specified interval.	True	
SIP_REG_ATTEMPTS	COUNTER	No	Current number of SIP registration attempts on a trunk group for the specified interval.	True	
SIP_REG_COMPLETIONS	COUNTER	No	Current number of SIP registrations that have successfully completed on a trunk group for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
CALLS_WITH_PSX_DIPS	COUNTER	No	The number of calls that made a PSX Dip during the interval (applies to ERE, ePSX and external ePSX).	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
TOTAL_PSX_DIPS	COUNTER	No	The total number of PSX dips for the specified interval (applies to ERE, ePSX and external ePSX). To see the number of calls which made PSX Dips during the interval, see CALLS_WITH_PSX_DIPS metric. Example During the specified interval, two calls made three dips each (due to call redirection, etc.) to the PSX. This is logged as: CALLS_WITH_PSX_DIPS = 2 and TOTAL_PSX_DIPS = 6. If calls do not involve redirection or other complex scenarios such as two-stage dialing and transfers, these two metrics can use the same value.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACTIVE_REGS	COUNTER	No	Interval number of active registrations on this trunk group.	True	
MAX_ACTIVE_REGS	GAUGE	No	Maximum active registrations on this trunk group (high-watermark achieved on this trunk group).	True	
CALL_LIMIT	GAUGE	No	CALL_LIMIT is the summation of TOTAL_CALLS_AVAILABLE, INBOUND_CALLS_USAGE, PRIORITY_CALL_USAGE, and OUTBOUND_CALLS_USAGE from NBS5200TrunkGroup StatusStats table (when it is not unlimited). Note CALL_LIMIT is different from the Call Limit configured at the SBC 5x00 device.	True	
ACTIVE_SUBS	COUNTER	No	Current number of active subscriptions on this trunk group.	True	
MAX_ACTIVE_SUBS	GAUGE	No	Maximum number of active subscriptions on this trunk group (high-watermark achieved on this trunk group).	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
PEAK_CALL_RATE	GAUGE	No	The current system peak call arrival rate.	True	
ONGOING_CALLS	INTEGER	No	Total number of ongoing calls (nonstable + stable) on this trunk group	True	
STABLE_CALLS	INTEGER	No	Total number of stable calls on this trunk group	True	
CALL_UPDATES	INTEGER	No	Total number of call updates on this trunk group	True	
EMERGENCY_STABLE_CALLS	INTEGER	No	Total number of stable emergency calls on this trunk group	True	
EMERGENCY_ONGOING_CALLS	INTEGER	No	Total number of emergency calls (stable + nonstable) on this trunk group	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

CallIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
ZNAME	STRING	Yes	The name of the address context zone.	False	N/A
NAME	STRING	Yes	The name of this trunk group.	False	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_IN_USAGE	COUNTER	No	The duration, in seconds, for which all inbound calls in a given interval are using the trunkgroup. This metric is derived using the formula: (total # of inbound calls on the TG) * (interval size) * 60	True	SUM
SUM_OUT_USAGE	COUNTER	No	The duration, in seconds, for which all outbound calls in a given interval are using the trunkgroup. This metric is derived using the formula: (total # of outbound calls on the TG) * (interval size) * 60.	True	SUM
SUM_IN_CALLS	COUNTER	No	Number of completed inbound calls on this trunk group for the specified interval.	True	SUM
SUM_OUT_CALLS	COUNTER	No	Number of completed outbound calls on this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_ATTEMPTS	COUNTER	No	Number of inbound call attempts on this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_ATTEMPTS	COUNTER	No	Number of outbound call attempts on this trunk group for the specified interval.	True	SUM
SUM_MAX_COMPLETED_CALLS	COUNTER	No	The maximum number of completed calls in the inbound and outbound direction for this peer group for the specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_CALL_SETUP_TIME	COUNTER	No	Total call setup time for all completed calls in inbound and outbound directions for this trunk group for specified interval measured in hundredths of a second.	True	SUM
SUM_CALL_SETUPS	COUNTER	No	Total number of calls setup but not necessarily completed in the inbound and outbound directions for this trunk group for the specified interval.	True	SUM
SUM_ROUTING_ATTEMPTS	COUNTER	No	The number of routing attempts for this trunk group for the specified interval. Each PSX dip can return up to 200 routes. The SBC selects routes based on a number of criteria such as CAC and bandwidth availability. In some cases, crankback/ route advance is needed if the first selected route fails. This metric counts the number of routes attempted before the call succeeded. If the first route succeeds, this counter = 1.	True	SUM
SUM_IN_BW_USAGE	COUNTER	No	Sum of bandwidth usage (expected data rate in bits per second multiplied by call duration in seconds) for every inbound call associated with this trunk group for the specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_OUT_BW_USAGE	COUNTER	No	Sum of bandwidth usage (expected data rate in bits per second multiplied by call duration in seconds) for every outbound call associated with this trunk group for the specified interval.	True	SUM
AVG_MAX_ACTIVE_BW_USAGE	GAUGE	No	The high water mark of BW usage in either direction associated with this peer group for the specified interval.	True	MEAN
SUM_CALLS_WITH_PKT_OUTAGE	COUNTER	No	Number of calls with a maximum packet outage whose duration exceeds the configured minimum for this trunk group for the specified interval.	True	SUM
SUM_CALLS_WITH_PKT_OUTAGE_AT_END	COUNTER	No	Number of calls whose maximum packet outage occurs at the end of the call for this trunk group for the specified interval.	True	SUM
SUM_TOTAL_PKT_OUTAGE	COUNTER	No	Summation of packet outage durations (in milliseconds) whose duration exceeds the configured minimum which is reported during the specified performance interval.	True	SUM
AVG_MAX_PKT_OUTAGE	GAUGE	No	The single longest maximum reported packet outage duration (in milliseconds) experienced during the specified performance interval for this peer group.	True	MEAN

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_POD_EVENTS	COUNTER	No	Number of Packet Outage Detection (POD) Events detected for this peer group for the specified interval.	True	SUM
SUM_PLAYOUT_BUFFER_GOOD	COUNTER	No	Number of calls with all sub-intervals reporting GOOD playout buffer quality for this trunk group for the specified interval.	True	SUM
SUM_PLAYOUT_BUFFER_ACCEPTABLE	COUNTER	No	Number of calls with all sub-intervals reporting ACCEPTABLE or better playout buffer quality for this trunk group for the specified interval.	True	SUM
SUM_PLAYOUT_BUFFER_POOR	COUNTER	No	Number of calls with all sub-intervals reporting POOR or better playout buffer quality for this trunk group for the specified interval.	True	SUM
SUM_PLAYOUT_BUFFER_UNACCEPTABLE	COUNTER	No	Number of calls with at least one sub-interval reporting UNACCEPTABLE playout buffer quality for this trunk group for the specified interval.	True	SUM
SUM_SIP_REG_ATTEMPTS	COUNTER	No	The current number of SIP registration attempts on a peer group for the specified interval.	True	SUM
SUM_SIP_REG_COMPLETIONS	COUNTER	No	The current number of SIP registrations that have successfully completed on a peer group for the specified interval.	True	SUM
SUM_CALLS_WITH_PSX_DIPS	COUNTER	No	The number of calls that made a PSX Dip during the interval (applies to ERE, ePSX and external ePSX).	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_TOTAL_PSX_DIPS	COUNTER	No	The total number of PSX dips for the specified interval (applies to ERE, ePSX and external ePSX). To see the number of calls which made PSX Dips during the interval, see CALLS_WITH_PSX_DIPS metric. Example During the specified interval, two calls made three dips each (due to call redirection, etc.) to the PSX. This is logged as: CALLS_WITH_PSX_DIPS = 2 and TOTAL_PSX_DIPS = 6. If calls do not involve redirection or other complex scenarios such as two-stage dialing and transfers, these two metrics can use the same value.	True	SUM
SUM_ACTIVE_REGS	COUNTER	No	The Interval number of active registrations on this peer group.	True	SUM
AVG_MAX_ACTIVE_REGS	GAUGE	No	The Interval number of maximum active registrations on this peer group (this is the high-watermark achieved on this peer group).	True	MEAN
SUM_ACTIVE_SUBS	COUNTER	No	The Interval number of active subscribe on this peer group.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_MAX_ACTIVE_SUBS	GAUGE	No	The Interval number of maximum active subscribe on this peer group (this is the high-watermark achieved on this peer group).	True	MEAN
AVG_PEAK_CALL_RATE	GAUGE	No	Peak call arrival rate within a specified interval on this trunk group.	True	MEAN
AVG_ONGOING_CALLS	INTEGER	No	Total On Going Calls (Non-Stable + Stable) on this trunk group.	True	MEAN
AVG_STABLE_CALLS	INTEGER	No	Total Stable Calls on this trunk group.	True	MEAN
AVG_CALL_UPDATES	INTEGER	No	Total Call Updates on this trunk group.	True	MEAN
AVG_EMERGENCY_STABLE_CALLS	INTEGER	No	Total Emergency Stable Calls on this trunk group.	True	MEAN
AVG_EMERGENCY_ONGOING_CALLS	INTEGER	No	Total Emergency Calls Stable + Non-Stable on this trunk group.	True	MEAN
AVG_CALL_LIMIT	GAUGE	No	The sum of TOTAL_CALLS_AVAILABLE, INBOUND_CALLS_USAGE, PRIORITY_CALL_USAGE, and OUTBOUND_CALLS_USAGE from NBS5200TrunkGroupStatusStats table.	True	MEAN
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

DiamNodeRfIntervalStatistics

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
DNAME	STRING	Yes	The name of this Diameter Node.	
NAME	STRING	Yes	The name of the peer.	
RF_SUCCESS	GAUGE	No	The count of successful ACR/ACA exchanged.	
RF_FAILED	GAUGE	No	The count of un-successful ACR/ACA exchanged.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

DnsGroupDnsServerStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	DNS Group - CLI
GNAME	STRING	Yes	The name of the address context group.	False	
IND	GAUGE	Yes	The DNS server statistics index for this address context.	False	
IP_ADDRESS	INETADDRESS	No	The IP address of the DNS server requested for the statistics data.	False	
QUERIES	GAUGE	No	The number of queries made by the DNS client to this DNS server.	False	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
TIMEOUTS	GAUGE	No	The number of timeouts resulting from the queries made by the DNSC client to this DNS server.	False	
ERRORS	GAUGE	No	The number of errors resulting from the queries made by the DNSC client to this DNS server.	False	
REFERRALS	GAUGE	No	The number of referrals resulting from the queries made by the DNSC client to this DNS server.	False	
TOTAL_TCP_CONNECTION	GAUGE	No	The number of tries for connecting to DNS server.	True	
TCP_CONNECTION_FAILED	GAUGE	No	The number of times SBC failed to connect to DNS server.	True	
TCP_CONNECTION_SUCCESS	GAUGE	No	The number of successful TCP connection to DNS server.	True	
TCP_CONNECTION_TORN_DOWN	GAUGE	No	The number of TCP connection torn down with DNS server.	True	
TCP_FALLBACK	GAUGE	No	The number of times tcp fallback with DNS server.	True	
EDNS_STATUS	INTEGER	No	The number of times tcp fallback with DNS server.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

DSP Stats

DspResDspCallIntervalStats

Column Name	Column Type	Index	Description	CLI Command Reference
SYSTEM_NAME	STRING	Yes	Name of the system.	Show Table System
NUM_CALL_NO_DSP_ALLOC_FAIL	COUNTER	No	Number of call was successful without DSP resource allocation failure during an interval.	
NUM_CALL_WITH_DSP_ALLOC_FAIL	COUNTER	No	Number of call was successful with DSP resource allocation failure during an interval.	
NUM_CALL_FAIL_NO_G729	COUNTER	No	Number of call failed due to lack of G729 DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_G729	COUNTER	No	Number of call fails due to reason other than lack G729 DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_G729	COUNTER	No	Number of call was successful even though lack of G729 DSP resource during an interval.	
NUM_CALL_FAIL_NO_G726	COUNTER	No	Number of call failed due to lack of G726 DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_G726	COUNTER	No	Number of call fails due to reason other than lack G726 DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_SUCCESS_NO_G726	COUNTER	No	Number of call was successful even though lack of G726 DSP resource during an interval.	
NUM_CALL_FAIL_NO_G711_PACKET	COUNTER	No	Number of call failed due to lack of G711 Packet DSP resource during an interval.	
NUM_CALL_FAIL_ON_G711_PACKET	COUNTER	No	Number of call fails due to reason other than lack G711 Packet DSP resource during an interval.	
NUM_CALL_NO_G711_PACKET	COUNTER	No	Number of call was successful even though lack of G711 Packet DSP resource during an interval.	
NUM_CALL_FAIL_NO_G723	COUNTER	No	Number of call failed due to lack of G723 DSP resource during an interval.	
NUM_CALL_FAIL_ON_G723	COUNTER	No	Number of call fails due to reason other than lack G723 DSP resource during an interval.	
NUM_CALL_NO_G723	COUNTER	No	Number of call was successful even though lack of G723 DSP resource during an interval.	
NUM_CALL_FAIL_NO_ILBC	COUNTER	No	Number of call failed due to lack of ILBC DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_ON_ILBC	COUNTER	No	Number of call fails due to reason other than lack ILBC DSP resource during an interval.	
NUM_CALL_NO_ILBC	COUNTER	No	Number of call was successful even though lack of ILBC DSP resource during an interval.	
NUM_CALL_FAIL_NO_EVRCB	COUNTER	No	Number of call failed due to lack of EVRCB0 DSP resource during an interval.	
NUM_CALL_FAIL_ON_EVRCB	COUNTER	No	Number of call fails due to reason other than lack EVRCB0 DSP resource during an interval.	
NUM_CALL_NO_EVRCB	COUNTER	No	Number of call was successful even though lack of EVRCB0 DSP resource during an interval.	
NUM_CALL_FAIL_NO_GSM	COUNTER	No	Number of call failed due to lack of AMRNB DSP resource during an interval.	
NUM_CALL_FAIL_ON_GSM	COUNTER	No	Number of call fails due to reason other than lack AMRNB DSP resource during an interval.	
NUM_CALL_NO_GSM	COUNTER	No	Number of call was successful even though lack of AMRNB DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_NO_AMRWB	COUNTER	No	Number of call failed due to lack of AMRWB DSP resource during an interval.	
NUM_CALL_FAIL_ON_AMRWB	COUNTER	No	Number of call fails due to reason other than lack AMRWB DSP resource during an interval.	
NUM_CALL_NO_AMRWB	COUNTER	No	Number of call was successful even though lack of AMRWB DSP resource during an interval.	
NUM_CALL_FAIL_NO_G722	COUNTER	No	Number of call failed due to lack of G722 DSP resource during an interval.	
NUM_CALL_FAIL_ON_G722	COUNTER	No	Number of call fails due to reason other than lack G722 DSP resource during an interval.	
NUM_CALL_NO_G722	COUNTER	No	Number of call was successful even though lack of G722 DSP resource during an interval.	
NUM_CALL_FAIL_NO_TONE	COUNTER	No	Number of call failed due to lack of TONE DSP resource during an interval.	
NUM_CALL_FAIL_ON_TONE	COUNTER	No	Number of call fails due to reason other than lack TONE DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_NO_TONE	COUNTER	No	Number of call was successful even though lack of TONE DSP resource during an interval.	
NUM_CALL_FAIL_NO_EVRC	COUNTER	No	Number of call failed due to lack of EVRC DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_EVRC	COUNTER	No	Number of call fails due to reason other than lack EVRC DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_EVRC	COUNTER	No	Number of call was successful even though lack of EVRC DSP resource during an interval.	
NUM_CALL_FAIL_NO_G7221	COUNTER	No	Number of call failed due to lack of G7221 DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_G7221	COUNTER	No	Number of call fails due to reason other than lack G7221 DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_G7221	COUNTER	No	Number of call was successful even though lack of G7221 DSP resource during an interval.	
NUM_CALL_FAIL_NO_EFR	COUNTER	No	Number of call failed due to lack of Efr DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_OTHER_ON_EFR	COUNTER	No	Number of call fails due to reason other than lack Efr DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_EFR	COUNTER	No	Number of call was successful even though lack of Efr DSP resource during an interval.	
NUM_CALL_FAIL_NO_OPUS	COUNTER	No	Number of call failed due to lack of OPUS DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_OPUS	COUNTER	No	Number of call fails due to reason other than lack of OPUS DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_OPUS	COUNTER	No	Number of call was successful even though lack of OPUS DSP resource during an interval.	
NUM_CALL_FAIL_NO_SILK8	COUNT	No	Number of calls failed due to lack of SILK_8 DSP resource.	
NUM_CALL_FAIL_OTHER_SILK8	COUNT	No	Number of calls failed due to reason other than lack of SILK_8 DSP resource.	
NUM_CALL_SUCCESS_NO_SILK8	COUNT	No	Number of calls successful even with lack of SILK_8 DSP resource.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_NO_SILK16	COUNT	No	Number of calls successful even with lack of SILK_8 DSP resource.	
NUM_CALL_FAIL_OTHER_SILK16	COUNT	No	Number of calls failed due to reason other than lack of SILK_16 DSP resource.	
NUM_CALL_SUCCESS_NO_SILK16	COUNT	No	Number of calls successful even with lack of SILK_16 DSP resource.	
NUM_CALL_FAIL_NO_EVS	INTEGER	No	The number of call fails due to the lack of EVS DSP resource during a time interval.	
NUM_CALL_FAIL_OTHER_EVS	INTEGER	No	The number of call fails due to a reason other than the lack of EVS DSP resource during a time interval.	
NUM_CALL_SUCCESS_NO_EVS	INTEGER	No	The number of calls was successful despite the lack of EVS DSP resource during a time interval.	
NUM_CALL_FAIL_L16	COUNT	False	The number of call failed due to lack of L16 DSP resource during a interval time.	
NUM_CALL_FAIL_OTHER_L16	COUNT	False	The number of call fails due to reason other than lack of L16 DSP resource during a interval time.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_SUCCESS_L16	COUNT	False	The number of call was successful even though lack of L16 DSP resource during a interval time.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

DspResDspCallIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SYSTEM_NAME	STRING	Yes	The name of the system.	False	N/A
SUM_NUM_CALL_NO_DSP_ALLOC_FAIL	COUNTER	No	The sum of the number of successful calls without DSP resource allocation failure during an interval.	True	SUM
SUM_NUM_CALL_WITH_DSP_ALLOC_FAIL	COUNTER	No	The sum of the number of successful calls with DSP resource allocation failure during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_G729	COUNTER	No	The sum of the number of calls failed due to lack of G729 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_ON_G729	COUNTER	No	The sum of the number of calls failed due to reason other than lack G729 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_G729	COUNTER	No	The sum of the number of successful calls even though lack of G729 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_G726	COUNTER	No	The sum of the number of calls failed due to lack of G726 DSP resource during an interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_FAIL_OTHER_ON_G726	COUNTER	No	The sum of the number of calls failed due to reason other than lack G726 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_G726	COUNTER	No	The sum of the number of successful calls even though lack of G726 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_G711_PACKET	COUNTER	No	The sum of the number of calls failed due to lack of G711 Packet DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_G711_PACKET	COUNTER	No	The sum of the number of calls failed due to reason other than lack G711 Packet DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_G711_PACKET	COUNTER	No	The sum of the number of successful calls even though lack of G711 Packet DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_G723	COUNTER	No	The sum of the number of calls failed due to lack of G723 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_G723	COUNTER	No	The sum of the number of calls failed due to reason other than lack G723 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_G723	COUNTER	No	The sum of the number of successful calls even though lack of G723 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_ILBC	COUNTER	No	The sum of the number of calls failed due to lack of ILBC DSP resource during an interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_FAIL_ON_ILBC	COUNTER	No	The sum of the number of calls failed due to reason other than lack ILBC DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_ILBC	COUNTER	No	The sum of the number of successful calls even though lack of ILBC DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_EVRCB	COUNTER	No	The sum of the number of calls failed due to lack of EVRCB0 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_EVRCB	COUNTER	No	The sum of the number of calls fails due to reason other than lack EVRCB0 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_EVRCB	COUNTER	No	The sum of the number of successful calls even though lack of EVRCB0 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_GSM	COUNTER	No	The sum of the number of calls failed due to lack of AMRNB DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_GSM	COUNTER	No	The sum of the number of calls failed due to reason other than lack AMRNB DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_GSM	COUNTER	No	The sum of the number of successful calls even though lack of AMRNB DSP resource during an interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_FAIL_NO_AMRWB	COUNTER	No	The sum of the number of calls failed due to lack of AMRWB DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_AMRWB	COUNTER	No	The sum of the number of calls failed due to reason other than lack AMRWB DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_AMRWB	COUNTER	No	The sum of the number of successful calls even though lack of AMRWB DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_G722	COUNTER	No	The sum of the number of calls failed due to lack of G722 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_G722	COUNTER	No	The sum of the number of calls failed due to reason other than lack G722 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_G722	COUNTER	No	The sum of the number of successful calls even though lack of G722 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_TONE	COUNTER	No	The sum of the number of calls failed due to lack of TONE DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_TONE	COUNTER	No	The sum of the number of calls failed due to reason other than lack TONE DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_TONE	COUNTER	No	The sum of the number of successful calls even though lack of TONE DSP resource during an interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_FAIL_NO_EVRC	COUNTER	No	The sum of the number of calls failed due to lack of EVRC DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_ON_EVRC	COUNTER	No	The sum of the number of calls failed due to reason other than lack EVRC DSP resource during an interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_EVRC	COUNTER	No	The sum of the number of successful calls even though lack of EVRC DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_EFR	COUNTER	No	The sum of the number of calls failed due to lack of Efr DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_ON_EFR	COUNTER	No	The sum of the number of calls failed due to reason other than lack Efr DSP resource during an interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_EFR	COUNTER	No	The sum of the number of successful calls even though lack of Efr DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_G7221	COUNTER	No	The sum of the number of calls failed due to lack of G7221 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_ON_G7221	COUNTER	No	The sum of the number of calls failed due to reason other than lack G7221 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_G7221	COUNTER	No	The sum of the number of successful calls even though lack of G7221 DSP resource during an interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_FAIL_NO_OPUS	COUNTER	No	The sum of the number of calls failed due to lack of OPUS DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_ON_OPUS	COUNTER	No	The sum of the number of calls failed due to reason other than lack of OPUS DSP resource during an interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_OPUS	COUNTER	No	The sum of the number of successful calls even though lack of OPUS DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_EVS	INTEGER	No	The sum of the number of calls failed due to the lack of EVS DSP resource during a time interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_EVS	INTEGER	No	The sum of the number of calls failed due to a reason other than the lack of EVS DSP resource during a time interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_EVS	INTEGER	No	The sum of the number of calls was successful despite the lack of EVS DSP resource during a time interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_SILK8	INTEGER	No	The sum of the number of calls failed due to lack of SILK_8 DSP resource.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_SILK8	INTEGER	No	The sum of the number of calls failed due to reason other than lack of SILK_8 DSP resource.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_SILK8	INTEGER	No	The sum of the number of calls successful even with lack of SILK_8 DSP resource.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_FAIL_NO_SILK16	INTEGER	No	The sum of the number of calls successful even with lack of SILK_8 DSP resource.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_SILK16	INTEGER	No	The sum of the number of calls failed due to reason other than lack of SILK_16 DSP resource.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_SILK16	INTEGER	No	The sum of the number of successful calls even with lack of SILK_16 DSP resource.	True	SUM
NUM_CALL_FAIL_L16	COUNT	False	The number of call failed due to lack of L16 DSP resource during a interval time.	True	SUM
NUM_CALL_FAIL_OTHER_L16	COUNT	False	The number of call fails due to reason other than lack of L16 DSP resource during a interval time.	True	SUM
NUM_CALL_SUCCESS_L16	COUNT	False	The number of call was successful even though lack of L16 DSP resource during a interval time.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

DspResDspUsageIntervalStats

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
SYSTEM_NAME	STRING	Yes	Name of the system.		Show Table System
G729_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G729 DSP pad during an interval time.		
G729_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G729 DSP pad during an interval time.		
G729_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G729 DSP pad during an interval time.		
G726_PEAK_USED_COUNT	GAUGE	No	The Interval number of Peak usage of type G726 DSP pad during an interval time.		
G726_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G726 DSP pad during an interval time.		
G726_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G726 DSP pad during an interval time.		
G711_PACKET_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711Packet DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711_PACKET_AVG_USED_COUNT	GAUGE	No	The average usage of type G711Packet DSP pad during an interval time.		
G711_PACKET_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711Packet DSP pad during an interval time.		
G723_PEAK_USED_COUNT	GAUGE	No	The Interval number of Peak usage of type G723 DSP pad during an interval time.		
G723_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G723 DSP pad during an interval time.		
G723_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G723 DSP pad during an interval time.		
ILBC_PEAK_USED_COUNT	GAUGE	No	The peak usage of type ILBC DSP pad during an interval time.		
ILBC_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type ILBC DSP pad during an interval time.		
ILBC_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type ILBC DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
EVRCB0_PEAK_USED_COUNT	GAUGE	No	The peak usage of type EVRCB0 DSP pad during an interval time.		
EVRCB0_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type EVRCB0 DSP pad during an interval time.		
EVRCB0_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type EVRCB0 DSP pad during an interval time.		
GSM_PEAK_USED_COUNT	GAUGE	No	The peak usage of type AMRNB DSP pad during an interval time.		
GSM_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type AMRNB DSP pad during an interval time.		
GSM_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type AMRNB DSP pad during an interval time.		
AMRWB_PEAK_USED_COUNT	GAUGE	No	The peak usage of type Amrwb DSP pad during an interval time.		
AMRWB_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type Amrwb DSP pad during an interval time.		
AMRWB_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type Amrwb DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G722_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 DSP pad during an interval time.		
G722_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G722 DSP pad during an interval time.		
G722_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G722 DSP pad during an interval time.		
TONE_PEAK_USED_COUNT	GAUGE	No	The peak usage of type TONE DSP pad during an interval time.		
TONE_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type TONE DSP pad during an interval time.		
TONE_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type TONE DSP pad during an interval time.		
EVRC_PEAK_USED_COUNT	GAUGE	No	The peak usage of type EVRCB0 DSP pad during an interval time.		
EVRC_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type EVRC DSP pad during an interval time.		
EVRC_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type EVRC DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G7221_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G7221 DSP pad during an interval time.		
G7221_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G7221 DSP pad during an interval time.		
G7221_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G7221 DSP pad during an interval time.		
EFR_PEAK_USED_COUNT	GAUGE	No	The peak usage of type Efr DSP pad during an interval time.		
EFR_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type Efr DSP pad during an interval time.		
EFR_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type Efr DSP pad during an interval time.		
G711SS_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711Ss DSP pad during an interval time.		
G711SS_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G711Ss DSP pad during an interval time.		
G711SS_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G711Ss DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G729V8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G729 V8 DSP pad during an interval time.		
G729V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G729 V8 DSP pad during an interval time.		
G729V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G729 V8 DSP pad during an interval time.		
G726V8_PEAK_USED_COUNT	GAUGE	No	The Interval number of Peak usage of type G726 V8 DSP pad during an interval time.		
G726V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G726 V8 DSP pad during an interval time.		
G726V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G726 V8 DSP pad during an interval time.		
G711V8_PACKET_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711Packet V8 DSP pad during an interval time.		
G711V8_PACKET_AVG_USED_COUNT	GAUGE	No	The average usage of type G711Packet V8 DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711V8_PACKET_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711Packet V8 DSP pad during an interval time.		
G711SSV8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711SSPacket V8 DSP pad during an interval time.		
G711SSV8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G711SSPacket V8 DSP pad during an interval time.		
G711SSV8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G711SSPacket V8 DSP pad during an interval time.		
G723V8_PEAK_USED_COUNT	GAUGE	No	The Interval number of Peak usage of type G723 V8 DSP pad during an interval time.		
G723V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G723 V8 DSP pad during an interval time.		
G723V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G723 V8 DSP pad during an interval time.		
ILBCV8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type ILBC V8 DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
ILBCV8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type ILBC V8 DSP pad during an interval time.		
ILBCV8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type ILBC V8 DSP pad during an interval time.		
G722V8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 V8 DSP pad during an interval time.		
G722V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G722 V8 DSP pad during an interval time.		
G722V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G722 V8 DSP pad during an interval time.		
G7221V8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722.1 V8 DSP pad during an interval time.		
G7221V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G722.1 V8 DSP pad during an interval time.		
G7221V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G722.1 V8 DSP pad during an interval time.		
OPUS_PEAK_USED_COUNT	GAUGE	No	The peak usage of type OPUS DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
OPUS_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type OPUS DSP pad during an interval time.		
OPUS_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type OPUS DSP pad during an interval time.		
EVS_PEAK_USED_COUNT	GAUGE	No	The peak usage of type EVS DSP pad during an interval time.		
EVS_AVG_USED_COUNT	GAUGE	No	The average usage of type EVS DSP pad during an interval time.		
EVS_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type EVS DSP pad during an interval time.		
SILK8_PEAK_USED_COUNT	COUNT	No	The peak usage of type SILK_8 DSP PAD.		
SILK8_AVG_USED_COUNT	COUNT	No	The average usage of type SILK_8 DSP PAD.		
SILK8_AVG_AVAIL_COUNT	COUNT	No	The average availability of type SILK_8 DSP PAD.		
SILK16_PEAK_USED_COUNT	COUNT	No	The peak usage of type SILK_16 DSP PAD.		
SILK16_AVG_USED_COUNT	COUNT	No	The average usage of type SILK_16 DSP PAD.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
SILK16_AVG_AVAIL_COUNT	COUNT	No	The average availability of type SILK_16 DSP PAD.		
AMRWT140_PEAK_USED_COUNT	COUNT	No	The peak usage of type AMR with T.140 DSP pad during an interval time.		
AMRWT140_AVG_USED_COUNT	COUNT	No	The peak usage of type AMR with T.140 DSP pad during an interval time.		
AMRWT140_AVG_AVAIL_COUNT	COUNT	No	The average availability of type AMR with T.140 DSP pad during an interval time.		
AMRWBT140_PEAK_USED_COUNT	COUNT	No	The peak usage of type AMRWB with T.140 DSP pad during an interval time.		
AMRWBT140_AVG_USED_COUNT	COUNT	No	The average usage of type SILK_16 DSP pad during an interval time.		
AMRWBT140_AVG_AVAIL_COUNT	COUNT	No	The average availability of type SILK_16 DSP pad during an interval time.		
AMR_PEAK_USAGE_COUNT	GAUGE	No	The current peak usage of type AMRNB DSP PAD.		
AMR_AVG_USAGE_COUNT	GAUGE	No	The current average usage of type AMRNB DSP PAD.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
AMR_AVG_A VAIL_COUNT	GAUGE	No	The current average availability of type AMRNB DSP PAD.		
EVS_T140_P EAK_USED_ COUNT	GAUGE	No	The peak usage of type EVS with T.140 DSP pad during an interval time.		
EVS_T140_A VERAGE_US ED_COUNT	GAUGE	No	The average usage of type EVS with T.140 DSP pad during an interval time.		
EVS_T140_A VERAGE_AVA IL_COUNT	GAUGE	No	The average availability of type EVS with T.140 DSP pad during an interval time.		
G711T140_PE AK_USED_C OUNT	GAUGE	No	The average availability of type EVS with T.140 DSP pad during an interval time.	MEAN	
G711T140_AV G_USED_CO UNT	GAUGE	No	The average usage of type G711 with T.140 DSP pad during an interval time.	MEAN	
G711T140_AV G_AVAIL_CO UNT	GAUGE	No	The average availability of type G711 with T.140 DSP pad during an interval time.	MEAN	
G711SST140_ PEAK_USED_ COUNT	GAUGE	No	The peak usage of type G711SS with T.140 DSP pad during an interval time.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SST140_AVG_USED_COUNT	GAUGE	No	The average usage of type G711SS with T.140 DSP pad during an interval time.	MEAN	
G711SST140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711SS with T.140 DSP pad during an interval time.	MEAN	
OPUST140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type Opus with T.140 DSP pad during an interval time.	MEAN	
OPUST140_AVG_USED_COUNT	GAUGE	No	The average usage of type Opus with T.140 DSP pad during an interval time.	MEAN	
OPUST140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type Opus with T.140 DSP pad during an interval time.	MEAN	
G722T140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 with T.140 DSP pad during an interval time.	MEAN	
G722T140_AVG_USED_COUNT	GAUGE	No	The average usage of type G722 with T.140 DSP pad during an interval time.	MEAN	
G722T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G722 with T.140 DSP pad during an interval time.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G722V8T140_ PEAK_USED_ COUNT	GAUGE	No	The peak usage of type G722 V8 with T.140 DSP pad during an interval time.	MEAN	
G722V8T140_ AVG_USED_ COUNT	GAUGE	No	The average usage of type G722 V8 with T.140 DSP pad during an interval time.	MEAN	
G722V8T140_ AVG_AVAIL_ COUNT	GAUGE	No	The average availability of type G722 V8 with T.140 DSP pad during an interval time.	MEAN	
G711T140V8_ PEAK_USED_ COUNT	GAUGE	No	The peak usage of type G711 V8 with T.140 DSP pad during an interval time.	MEAN	
G711T140V8_ AVG_USED_ COUNT	GAUGE	No	The average usage of type G711 V8 with T.140 DSP pad during an interval time.	MEAN	
G711T140V8_ AVG_AVAIL_ COUNT	GAUGE	No	The average availability of type G711 V8 with T.140 DSP pad during an interval time.	MEAN	
G711SSV8T140_ PEAK_USED_ COUNT	GAUGE	No	The peak usage of type G711SS V8 with T.140 DSP pad during an interval time.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SSV8T140_AVG_USAGE_COUNT	GAUGE	No	The average usage of type G711SS V8 with T.140 DSP pad during an interval time.	MEAN	
G711SSV8T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711SS V8 with T.140 DSP pad during an interval time.	MEAN	
L16_PEAK_USAGE_COUNT	GAUGE	No	The peak usage of type L16 DSP pad during an interval time.	MEAN	
L16_AVG_USAGE_COUNT	GAUGE	No	The average usage of type L16 DSP pad during an interval time.	MEAN	
L16_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type L16 DSP pad during an interval time.	MEAN	
CE_NAME	STRING	No	The name of the compute element for this entry.	N/A	

DspResDspUsageIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SYSTEM_NAME	STRING	Yes	Name of the system.	False	N/A
AVG_G729_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G729 DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_G729_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G729 DSP pad during an interval time.	True	AVG
AVG_G729_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G729 DSP pad during an interval time.	True	AVG
AVG_G726_PEAK_USED_COUNT	GAUGE	No	The average of interval number of Peak usage of type G726 DSP pad during an interval time.i	True	AVG
AVG_G726_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G726 DSP pad during an interval time.	True	AVG
AVG_G726_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G726 DSP pad during an interval time.	True	AVG
AVG_G711_PACKET_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G711Packet DSP pad during an interval time.	True	AVG
AVG_G711_PACKET_AVG_USED_COUNT	GAUGE	No	The average of average usage of type G711Packet DSP pad during an interval time.	True	AVG
AVG_G711_PACKET_AVG_AVAIL_COUNT	GAUGE	No	The average of average availability of type G711Packet DSP pad during an interval time.	True	AVG
AVG_G723_PEAK_USED_COUNT	GAUGE	No	The average of interval number of Peak usage of type G723 DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_G723_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G723 DSP pad during an interval time.	True	AVG
AVG_G723_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G723 DSP pad during an interval time.	True	AVG
AVG_ILBC_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type ILBC DSP pad during an interval time.	True	AVG
AVG_ILBC_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type ILBC DSP pad during an interval time.	True	AVG
AVG_ILBC_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type ILBC DSP pad during an interval time.	True	AVG
AVG_EVRCB0_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type EVRCB0 DSP pad during an interval time.	True	AVG
AVG_EVRCB0_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type EVRCB0 DSP pad during an interval time.	True	AVG
AVG_EVRCB0_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type EVRCB0 DSP pad during an interval time.	True	AVG
AVG_GSM_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type AMRNB DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_GSM_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type AMRNB DSP pad during an interval time.	True	AVG
AVG_GSM_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type AMRNB DSP pad during an interval time.	True	AVG
AVG_AMRWB_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type Amrwb DSP pad during an interval time.	True	AVG
AVG_AMRWB_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type Amrwb DSP pad during an interval time.	True	AVG
AVG_AMRWB_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type Amrwb DSP pad during an interval time.	True	AVG
AVG_G722_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G722 DSP pad during an interval time.	True	AVG
AVG_G722_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G722 DSP pad during an interval time.	True	AVG
AVG_G722_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G722 DSP pad during an interval time.	True	AVG
AVG_TONE_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type TONE DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_TONE_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type TONE DSP pad during an interval time.	True	AVG
AVG_TONE_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type TONE DSP pad during an interval time.	True	AVG
AVG_EVRC_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type EVRCB0 DSP pad during an interval time.	True	AVG
AVG_EVRC_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type EVRC DSP pad during an interval time.	True	AVG
AVG_EVRC_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type EVRC DSP pad during an interval time.	True	AVG
AVG_G7221_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G7221 DSP pad during an interval time.	True	AVG
AVG_G7221_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G7221 DSP pad during an interval time.	True	AVG
AVG_G7221_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G7221 DSP pad during an interval time.	True	AVG
AVG_EFR_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type Efr DSP pad during an interval time.	True	AVG
AVG_EFR_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type Efr DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_EFR_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type Efr DSP pad during an interval time.	True	AVG
AVG_G711SS_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G711Ss DSP pad during an interval time.	True	AVG
AVG_G711SS_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G711Ss DSP pad during an interval time.	True	AVG
AVG_G711SS_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G711Ss DSP pad during an interval time.	True	AVG
AVG_G729V8_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G729 V8 DSP pad during an interval time.	True	AVG
AVG_G729V8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G729 V8 DSP pad during an interval time.	True	AVG
AVG_G729V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G729 V8 DSP pad during an interval time.	True	AVG
AVG_G726V8_PEAK_USED_COUNT	GAUGE	No	The average of interval number of Peak usage of type G726 V8 DSP pad during an interval time.	True	AVG
AVG_G726V8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G726 V8 DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_G726V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G726 V8 DSP pad during an interval time.	True	AVG
AVG_G711V8_PACKET_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G711Packet V8 DSP pad during an interval time.	True	AVG
AVG_G711V8_PACKET_AVG_USED_COUNT	GAUGE	No	The average of average usage of type G711Packet V8 DSP pad during an interval time.	True	AVG
AVG_G711V8_PACKET_AVG_AVAIL_COUNT	GAUGE	No	The average of average availability of type G711Packet V8 DSP pad during an interval time.	True	AVG
AVG_G711SSV8_PACKET_USED_COUNT	GAUGE	No	The average of peak usage of type G711SSPacket V8 DSP pad during an interval time.	True	AVG
AVG_G711SSV8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G711SSPacket V8 DSP pad during an interval time.	True	AVG
AVG_G711SSV8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G711SSPacket V8 DSP pad during an interval time.	True	AVG
AVG_G723V8_PACKET_USED_COUNT	GAUGE	No	The average of interval number of Peak usage of type G723 V8 DSP pad during an interval time.	True	AVG
AVG_G723V8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G723 V8 DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_G723V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G723 V8 DSP pad during an interval time.	True	AVG
AVG_ILBCV8_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type ILBC V8 DSP pad during an interval time.	True	AVG
AVG_ILBCV8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type ILBC V8 DSP pad during an interval time.	True	AVG
AVG_ILBCV8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type ILBC V8 DSP pad during an interval time.	True	AVG
AVG_G722V8_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G722 V8 DSP pad during an interval time.	True	AVG
AVG_G722V8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G722 V8 DSP pad during an interval time.	True	AVG
AVG_G722V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G722 V8 DSP pad during an interval time.	True	AVG
AVG_G7221V8_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G722.1 V8 DSP pad during an interval time.	True	AVG
AVG_G7221V8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G722.1 V8 DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_G7221V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G722.1 V8 DSP pad during an interval time.	True	AVG
AVG_OPUS_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type OPUS DSP pad during an interval time.	True	AVG
AVG_OPUS_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type OPUS DSP pad during an interval time.	True	AVG
AVG_OPUS_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type OPUS DSP pad during an interval time.	True	AVG
AVG_EVS_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type EVS DSP pad during an interval time.	True	AVG
AVG_EVS_AVG_USED_COUNT	GAUGE	No	The average of average usage of type EVS DSP pad during an interval time.	True	AVG
AVG_EVS_AVG_AVAIL_COUNT	GAUGE	No	The average of average availability of type EVS DSP pad during an interval time.	True	AVG
AVG_SILK8_PEAK_USED_COUNT	COUNT	No	The average of peak usage of type SILK_8 DSP PAD.	True	AVG
AVG_SILK8_AVG_USED_COUNT	COUNT	No	The average of average usage of type SILK_8 DSP PAD.	True	AVG
AVG_SILK8_AVG_AVAIL_COUNT	COUNT	No	The average of average availability of type SILK_8 DSP PAD.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_SILK16_PEAK_USED_COUNT	COUNT	No	The average of peak usage of type SILK_16 DSP PAD.	True	AVG
AVG_SILK16_AVG_USED_COUNT	COUNT	No	The average of average usage of type SILK_16 DSP PAD.	True	AVG
AVG_SILK16_AVG_AVAIL_COUNT	COUNT	No	The average of average availability of type SILK_16 DSP PAD.	True	AVG
AVG_AMRWT140_PEAK_USED_COUNT	COUNT	No	The average of peak usage of type AMR with T.140 DSP pad during an interval time.	True	AVG
AVG_AMRWT140_AVG_USED_COUNT	COUNT	No	The average of average usage of type AMR with T.140 DSP pad during an interval time.	True	AVG
AVG_AMRWT140_AVG_AVAIL_COUNT	COUNT	No	The average of average availability of type AMR with T.140 DSP pad during an interval time.	True	AVG
AVG_AMRWBT140_PEAK_USED_COUNT	COUNT	No	The average of peak usage of type AMRWB with T.140 DSP pad during an interval time.	True	AVG
AVG_AMRWBT140_AVG_USED_COUNT	COUNT	No	The average of average usage of type SILK_16 DSP pad during an interval time.	True	AVG
AVG_AMRWBT140_AVG_AVAIL_COUNT	COUNT	No	The average of average availability of type SILK_16 DSP pad during an interval time.	True	AVG
AVG_AMR_PEAK_USAGE_COUNT	GAUGE	No	The current peak usage of type AMRNB DSP PAD.	True	MEAN

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_AMR_AVG_USAGE_COUNT	GAUGE	No	The current average usage of type AMRNB DSP PAD.	True	MEAN
AVG_AMR_AVG_AVAIL_COUNT	GAUGE	False	The current average availability of type AMRNB DSP PAD.	True	MEAN
EVS_T140_PEAK_USED_COUNT	GAUGE	False	The peak usage of type EVS with T.140 DSP pad during an interval time.	False	MEAN
EVS_T140_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type EVS with T.140 DSP pad during an interval time.	False	MEAN
EVS_T140_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type EVS with T.140 DSP pad during an interval time.	False	MEAN
L16_PEAK_USED_COUNT	GAUGE	False	The peak usage of type L16 DSP pad during an interval time.	True	MEAN
L16_AVG_USED_COUNT	GAUGE	False	The average usage of type L16 DSP pad during an interval time.	True	MEAN
L16_AVG_AVAIL_COUNT	GAUGE	False	The average availability of type L16 DSP pad during an interval time.	True	MEAN
G711T140_PEAK_USED_COUNT	GAUGE	No	The average availability of type EVS with T.140 DSP pad during an interval time.	True	MEAN
G711T140_AVG_USAGE_COUNT	GAUGE	No	The average usage of type G711 with T.140 DSP pad during an interval time.	True	MEAN
G711T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711 with T.140 DSP pad during an interval time.	True	MEAN

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
G711SST140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711SS with T.140 DSP pad during an interval time.	True	MEAN
G711SST140_AVG_USED_COUNT	GAUGE	No	The average usage of type G711SS with T.140 DSP pad during an interval time.	True	MEAN
G711SST140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711SS with T.140 DSP pad during an interval time.	True	MEAN
OPUST140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type Opus with T.140 DSP pad during an interval time.	True	MEAN
OPUST140_AVG_USED_COUNT	GAUGE	No	The average usage of type Opus with T.140 DSP pad during an interval time.	True	MEAN
OPUST140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type Opus with T.140 DSP pad during an interval time.	True	MEAN
G722T140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 with T.140 DSP pad during an interval time.	True	MEAN
G722T140_AVG_USED_COUNT	GAUGE	No	The average usage of type G722 with T.140 DSP pad during an interval time.	True	MEAN
G722T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G722 with T.140 DSP pad during an interval time.	True	MEAN
G722V8T140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 V8 with T.140 DSP pad during an interval time.	True	MEAN

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
G722V8T140_AVG_USED_COUNT	GAUGE	No	The average usage of type G722 V8 with T.140 DSP pad during an interval time.	True	MEAN
G722V8T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G722 V8 with T.140 DSP pad during an interval time.	True	MEAN
G711T140V8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711 V8 with T.140 DSP pad during an interval time.	True	MEAN
G711T140V8_AVG_USED_COUNT	GAUGE	No	The average usage of type G711 V8 with T.140 DSP pad during an interval time.	True	MEAN
G711T140V8_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711 V8 with T.140 DSP pad during an interval time.	True	MEAN
G711SSV8T140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711SS V8 with T.140 DSP pad during an interval time.	True	MEAN
G711SSV8T140_AVG_USED_COUNT	GAUGE	No	The average usage of type G711SS V8 with T.140 DSP pad during an interval time.	True	MEAN
G711SSV8T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711SS V8 with T.140 DSP pad during an interval time.	True	MEAN
L16_PEAK_USED_COUNT	GAUGE	No	The peak usage of type L16 DSP pad during an interval time.	True	MEAN
L16_AVG_USED_COUNT	GAUGE	No	The average usage of type L16 DSP pad during an interval time.	True	MEAN

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
L16_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type L16 DSP pad during an interval time.	True	MEAN
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

EthernetPortMgmtStats

Column Name	Column Type	Index	Description	CLI Command Reference
PORT_NAME	STRING	Yes	The name of this port.	Ethernet Port - CLI
RX_PACKETS	COUNTER64	No	The number of received packets.	
TX_PACKETS	COUNTER64	No	The number of transmitted packets.	
RX_ERRORS	COUNTER	No	The number of bad packets received.	
TX_ERRORS	COUNTER	No	The number of packet transmit failures.	
RX_DROPPED	COUNTER	No	The number of packets dropped due to no receive buffers.	
TX_DROPPED	COUNTER	No	The number of packets dropped due to no transmit buffers.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

EthernetPortPacketStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
PORT_NAME	STRING	Yes	The name of this port.	True	Ethernet Port - CLI

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
RX_PACKETS	COUNTER64	No	The number of received packets.	True	
TX_PACKETS	COUNTER64	No	The number of transmitted packets.	True	
RX_ERRORS	COUNTER	No	The number of bad packets received.	True	
TX_ERRORS	COUNTER	No	The number of packet transmit failures.	True	
RX_DROPPE D	COUNTER	No	The number of packets dropped due to no receive buffers.	True	
TX_DROPPE D	COUNTER	No	The number of packets dropped due to no transmit buffers.	True	
RX_BYTES	COUNTER64	No	The number of received bytes.	True	
TX_BYTES	COUNTER64	No	The number of transmitted bytes.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

H323SigPortStatisticsStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context zone.	

Column Name	Column Type	Index	Description	CLI Command Reference
NAME	STRING	Yes	The name of this H.323 Signaling Port.	
IND	GAUGE	Yes	The index of this H.323 Signaling Port.	
STATUS	INTEGER	No	Status of the H.323 Signaling Port.	
INGRESS_CALLS_COMPLETED	INTEGER	No	Number of Ingress calls completed since system boot up.	
EGRESS_CALLS_COMPLETED	INTEGER	No	Number of Egress calls completed since system boot up.	
INGRESS_CALLS_ATTEMPTED	INTEGER	No	Number of Ingress calls attempted since system boot up.	
EGRESS_CALLS_ATTEMPTED	INTEGER	No	Number of Egress calls attempted since system boot up.	
H225_MESSAGES_SENT	COUNTER64	No	Number of H.225 messages that sent since system boot up.	
H225_MESSAGE_BYTES_SENT	COUNTER64	No	Number of bytes of H.225 messages that sent since system boot up.	
H225_MESSAGES_RCVD	COUNTER64	No	Number of H.225 messages that are received since system boot up.	
H225_MESSAGE_BYTES_RCVD	COUNTER64	No	Number of bytes of H.225 messages that are received since system boot up.	
H245_MESSAGES_SENT	COUNTER64	No	Number of H.245 messages that sent since system boot up.	

Column Name	Column Type	Index	Description	CLI Command Reference
H245_MESSAGE_BYTES_SENT	COUNTER64	No	Number of bytes of H.245 messages that sent since system boot up.	
H245_MESSAGES_RCVD	COUNTER64	No	Number of H.245 messages that are received since system boot up.	
H245_MESSAGE_BYTES_RCVD	COUNTER64	No	Number of bytes of H.245 messages that are received since system boot up.	
ACTIVE_CALLS	INTEGER	No	Number of Active calls at this moment.	
H225_TCP_PORTS_OPENED	INTEGER	No	Number of H.225 TCP ports opened at this moment.	
H245_TCP_PORTS_OPENED	INTEGER	No	Number of H.245 TCP ports opened at this moment.	
H245_TCP_PORTS_ALLOCATED	INTEGER	No	Number of H.245 TCP ports allocated at this moment.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

IcmpGeneralGroupStats

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	The name of the compute element for this entry.	NA
IN_MSGS	COUNTER	No	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.	

Column Name	Column Type	Index	Description	CLI Command Reference
IN_ECHOS	COUNTER	No	The number of ICMP Echo (request) messages received.	
IN_ECHO_REPS	COUNTER	No	The number of ICMP Echo Reply messages received.	
IN_DEST_UNREACHS	COUNTER	No	The number of ICMP Destination Unreachable messages received.	
IN_ERRORS	COUNTER	No	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (such as, bad ICMP checksums, bad length).	
OUT_MSGS	COUNTER	No	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.	
OUT_ERRORS	COUNTER	No	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations, any type of error that contributes to the value of this counter may not exist.	
OUT_ECHOS	COUNTER	No	The number of ICMP Echo (request) messages sent.	
OUT_ECHO_REPS	COUNTER	No	The number of ICMP Echo Reply messages sent.	

Column Name	Column Type	Index	Description	CLI Command Reference
OUT_DEST_UN REACHS	COUNTER	No	The number of ICMP Destination Unreachable messages sent.	

Ip Stats

IpAclOverallStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	IP Access Control List - Non-Cloud - CLI
NAME	IMPLIEDSTRING	Yes	The name of the address context.	
MATCHED_NO_RULE	COUNTER	No	The number of times no rule is matched.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

IpAclOverallStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
NAME	IMPLIEDSTRING	Yes	The name of the address context.	False	N/A
SUM_MATCHED_NO_RULE	COUNTER	No	The sum of the number of times no rule is matched.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

IpAclRuleStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	IP Access Control List - Non-Cloud - CLI
NAME	STRING	Yes	The name of this IP access control list rule.	
MATCHES	COUNTER	No	The number of times this rule is matched.	
POLICER_DISCARDS	COUNTER	No	The number of times the policer for this rule discarded packets.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

IpAclRuleStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
NAME	STRING	Yes	The name of this IP access control list rule.	False	N/A
SUM_MATCHES	COUNTER	No	The sum of the number of times this rule is matched.	True	SUM
SUM_POLICER_DISCARDS	COUNTER	No	The sum of the number of times the policer for this rule discarded packets.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

IpGeneralGroupStats

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	The name of the compute element for this entry.	NA

Column Name	Column Type	Index	Description	CLI Command Reference
IN_RECEIVES	COUNTER	No	The total number of input datagrams received from interfaces, including those received in error.	
IN_HDR_ERRORS	COUNTER	No	The number of input datagrams discarded due to errors such as errors in IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options.	
IN_ADDR_ERRORS	COUNTER	No	The number of input datagrams discarded because the IP address in the destination field of the IP header was not a valid address for this entity to receive. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP routers and do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.	
IN_UNKNOWN_PROTOS	COUNTER	No	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.	

Column Name	Column Type	Index	Description	CLI Command Reference
IN_DISCARDS	COUNTER	No	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.	
IN_DELIVERS	COUNTER	No	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).	
OUT_REQUESTS	COUNTER	No	The total number of IP datagrams which local IP user- protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.	
OUT_DISCARDS	COUNTER	No	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter includes datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.	

Column Name	Column Type	Index	Description	CLI Command Reference
OUT_NO_ROUTE	COUNTER	No	The number of IP datagrams discarded because no route could transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this no-route criterion. This also includes any datagrams which a host cannot route because all of its default routers are down.	
REASM_TIMEOUT	INTEGER	No	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.	
REASM_REQDS	COUNTER	No	The number of IP fragments received that this entity needs to reassemble.	
REASM_OKS	COUNTER	No	The number of IP datagrams successfully re-assembled.	
REASM_FAILS	COUNTER	No	The number of failures detected by the IP re-assembly algorithm (for reasons such as timed out, errors). Note that this is not necessarily a count of discarded IP fragments since some algorithms (like the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.	
FRAG_OKS	COUNTER	No	The number of IP datagrams successfully fragmented at this entity.	
FRAG_FAILS	COUNTER	No	The number of IP datagrams discarded because this entity must, but cannot, fragment the IP datagrams. For example, because their Don't Fragment flag was set.	

IpPolicingSystemIntStats

Column Name	Column Type	Index	Description	CLI Command Reference
SYSTEM_NAME	STRING	Yes	Name of the system.	IP Policing - CLI
BAD_HDR_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the bad Ethernet/IP Header policer.	
BAD_HDR_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the bad Ethernet/IP Header policer.	
BAD_HDR_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the bad Ethernet/IP Header policer.	
BAD_HDR_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the bad Ethernet/IP Header policer.	
BAD_HDR_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the bad Ethernet/IP Header policer.	
BAD_HDR_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the bad Ethernet/IP Header policer.	
ARP_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the ARP policer.	
ARP_ACCEPT_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the ARP policer.	

Column Name	Column Type	Index	Description	CLI Command Reference
ARP_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the ARP policer.	
ARP_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the ARP policer.	
ARP_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the ARP policer.	
ARP_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the ARP policer.	
ARP_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the ARP policer.	
UFLOW_DISCARDED_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the micro flow policer.	
UFLOW_ACCEPTED_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the micro flow policer.	
UFLOW_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the micro flow policer.	
UFLOW_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the micro flow policer.	
UFLOW_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the micro flow policer.	
UFLOW_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the micro flow policer.	

Column Name	Column Type	Index	Description	CLI Command Reference
UFLOW_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the micro flow policer.	
ACL_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the access control list policer.	
ACL_ACCEPT_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the access control list policer.	
ACL_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the access control list policer.	
ACL_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the access control list policer.	
ACL_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the access control list policer.	
ACL_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the access control list policer.	
ACL_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the access control list policer.	
AGGREGATE_DISCARD_PKT_COUNT	COUNTER64	No	The current number of discarded packets for the aggregate policer.	
AGGREGATE_ACCEPT_PKT_COUNT	COUNTER64	No	The current number of discarded packets for the aggregate policer.	

Column Name	Column Type	Index	Description	CLI Command Reference
AGGREGATE_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the aggregate policer.	
AGGREGATE_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the aggregate policer.	
AGGREGATE_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the aggregate policer.	
AGGREGATE_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the aggregate policer.	
AGGREGATE_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the aggregate policer.	
IP_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the IPSEC Decrypt policer.	
IP_ACCEPT_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the IPSEC Decrypt policer.	
IP_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the IPSEC Decrypt policer.	
IP_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the IPSEC Decrypt policer.	
IP_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the IPSEC Decrypt policer.	

Column Name	Column Type	Index	Description	CLI Command Reference
IP_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the IPSEC Decrypt policer.	
IP_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the IPSEC Decrypt policer.	
MEDIA_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the media policer.	
MEDIA_ACCEPT_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the media policer.	
MEDIA_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the media policer.	
MEDIA_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the media policer.	
MEDIA_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the media policer.	
MEDIA_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the media policer.	
MEDIA_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the media policer.	
ROGUE_MEDIA_DISCARD_PKT_COUNT	COUNTER64	No	The current number of discarded packets for the rogue media policer.	
ROGUE_MEDIA_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the rogue media policer.	

Column Name	Column Type	Index	Description	CLI Command Reference
ROGUE_MEDIA_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the rogue media policer.	
ROGUE_MEDIA_MINOR_ALARM_DUR	COUNTER	No	The current duration of the minor alarms in seconds for the rogue media policer.	
ROGUE_MEDIA_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the rogue media policer.	
ROGUE_MEDIA_MAJOR_ALARM_DUR	COUNTER	No	The current duration of the major alarms in seconds for the rogue media policer.	
DISCARD_RULE_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the IPSEC Decrypt policer.	
DISCARD_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the discard rule.	
DISCARD_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the discard rule.	
DISCARD_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the discard rule.	
DISCARD_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the discard rule.	
DISCARD_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the discard rule.	

Column Name	Column Type	Index	Description	CLI Command Reference
DECRYPT_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of packets discarded by SRTP decrypt discards.	
PEAK_DECRYPT_DISCARD_RATE	GAUGE	No	The current peak discard rate for SRTP decrypt discards.	
MINOR_DECRYPT_ALARM_COUNT	INTEGER	No	The current number of minor alarms for SRTP decrypt discards.	
MINOR_DECRYPT_ALARM_DURATION	INTEGER	No	The current duration of the minor alarms in seconds for SRTP decrypt discards.	
MAJOR_DECRYPT_ALARM_COUNT	INTEGER	No	The current number of major alarms for the SRTP decrypt discards.	
MAJOR_DECRYPT_ALARM_DURATION	INTEGER	No	The current duration of the major alarms in seconds for SRTP decrypt discards.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

IpPolicingSystemIntStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SYSTEM_NAME	STRING	Yes	Name of the system.	False	N/A
AVG_BAD_HDR_DISCARD_PACKET_COUNT	COUNTER64	No	The average of current number of discarded packets for the bad Ethernet/IP Header policer.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_BAD_HDR_DISCARD_PACKET_COUNT	COUNTER64	No	The sum of current number of discarded packets for the bad Ethernet/IP Header policer.	True	SUM
AVG_BAD_HDR_PEAK_DISCARD_RATE	GAUGE	No	The average of current peak discard rate for the bad Ethernet/IP Header policer.	True	AVG
SUM_BAD_HDR_PEAK_DISCARD_RATE	GAUGE	No	The sum of current peak discard rate for the bad Ethernet/IP Header policer.	True	SUM
AVG_BAD_HDR_MINOR_ALARM_COUNT	COUNTER	No	The average of current number of minor alarms for the bad Ethernet/IP Header policer.	True	AVG
SUM_BAD_HDR_MINOR_ALARM_COUNT	COUNTER	No	The sum of current number of minor alarms for the bad Ethernet/IP Header policer.	True	SUM
AVG_BAD_HDR_MINOR_ALARM_DURATION	COUNTER	No	The average of current duration of the minor alarms in seconds for the bad Ethernet/IP Header policer.	True	AVG
SUM_BAD_HDR_MINOR_ALARM_DURATION	COUNTER	No	The sum of current duration of the minor alarms in seconds for the bad Ethernet/IP Header policer.	True	SUM
AVG_BAD_HDR_MAJOR_ALARM_COUNT	COUNTER	No	The average of current number of major alarms for the bad Ethernet/IP Header policer.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM__BAD_HDR_MAJOR_ALARM_COUNT	COUNTER	No	The sum of current number of major alarms for the bad Ethernet/IP Header policer.	True	SUM
AVG_BAD_HDR_MAJOR_ALARM_DURATION	COUNTER	No	The average of current duration of the major alarms in seconds for the bad Ethernet/IP Header policer.	True	AVG
SUM_BAD_HDR_MAJOR_ALARM_DURATION	COUNTER	No	The sum of current duration of the major alarms in seconds for the bad Ethernet/IP Header policer.	True	SUM
AVG_ARP_DISCARD_PACKET_COUNT	COUNTER64	No	The average of current number of discarded packets for the ARP policer.	True	AVG
SUM_ARP_DISCARD_PACKET_COUNT	COUNTER64	No	The sum of current number of discarded packets for the ARP policer.	True	SUM
AVG_ARP_ACCEPT_PACKET_COUNT	COUNTER64	No	The average of current number of discarded packets for the ARP policer.	True	AVG
SUM_ARP_ACCEPT_PACKET_COUNT	COUNTER64	No	The sum of current number of discarded packets for the ARP policer.	True	SUM
AVG_ARP_PEAK_DISCARD_RATE	GAUGE	No	The average of current peak discard rate for the ARP policer.	True	AVG
SUM_ARP_PEAK_DISCARD_RATE	GAUGE	No	The average of current peak discard rate for the ARP policer.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_ARP_MINOR_ALARM_COUNT	COUNTER	No	The average of current number of minor alarms for the ARP policer.	True	AVG
SUM_ARP_MINOR_ALARM_COUNT	COUNTER	No	The average of current number of minor alarms for the ARP policer.	True	SUM
AVG_ARP_MINOR_ALARM_DURATION	COUNTER	No	The average of current duration of the minor alarms in seconds for the ARP policer.	True	AVG
SUM_ARP_MINOR_ALARM_DURATION	COUNTER	No	The sum of current duration of the minor alarms in seconds for the ARP policer.	True	SUM
AVG_ARP_MAJOR_ALARM_COUNT	COUNTER	No	The average of current number of major alarms for the ARP policer.	True	AVG
SUM_ARP_MAJOR_ALARM_COUNT	COUNTER	No	The sum of current number of major alarms for the ARP policer.	True	SUM
AVG_ARP_MAJOR_ALARM_DURATION	COUNTER	No	The average of current duration of the major alarms in seconds for the ARP policer.	True	AVG
SUM_ARP_MAJOR_ALARM_DURATION	COUNTER	No	The sum of current duration of the major alarms in seconds for the ARP policer.	True	SUM
AVG_UFLOW_DISCARD_PACKET_COUNT	COUNTER64	No	The average of current number of discarded packets for the micro flow policer.	True	AVG
SUM_UFLOW_DISCARD_PACKET_COUNT	COUNTER64	No	The sum of current number of discarded packets for the micro flow policer.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_UFLOW_ACCEPT_PACKET_COUNT	COUNTER64	No	The average of current number of discarded packets for the micro flow policer.	True	AVG
SUM_UFLOW_ACCEPT_PACKET_COUNT	COUNTER64	No	The sum of current number of discarded packets for the micro flow policer.	True	SUM
AVG_UFLOW_PEAK_DISCARD_RATE	GAUGE	No	The average of current peak discard rate for the micro flow policer.	True	AVG
SUM_UFLOW_PEAK_DISCARD_RATE	GAUGE	No	The sum of current peak discard rate for the micro flow policer.	True	SUM
AVG_UFLOW_MINOR_ALARM_COUNT	COUNTER	No	The average of current number of minor alarms for the micro flow policer.	True	AVG
SUM_UFLOW_MINOR_ALARM_COUNT	COUNTER	No	The sum of current number of minor alarms for the micro flow policer.	True	SUM
AVG_UFLOW_MINOR_ALARM_DURATION	COUNTER	No	The average of current duration of the minor alarms in seconds for the micro flow policer.	True	AVG
SUM_UFLOW_MINOR_ALARM_DURATION	COUNTER	No	The sum of current duration of the minor alarms in seconds for the micro flow policer.	True	SUM
AVG_UFLOW_MAJOR_ALARM_COUNT	COUNTER	No	The average of current number of major alarms for the micro flow policer.	True	AVG
SUM_UFLOW_MAJOR_ALARM_COUNT	COUNTER	No	The sum of current number of major alarms for the micro flow policer.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_UFLOW_MAJOR_ALARM_DURATION	COUNTER	No	The average of current duration of the major alarms in seconds for the micro flow policer.	True	AVG
SUM_UFLOW_MAJOR_ALARM_DURATION	COUNTER	No	The sum of current duration of the major alarms in seconds for the micro flow policer.	True	SUM
AVG_ACL_DISCARDED_PACKET_COUNT	COUNTER64	No	The average of current number of discarded packets for the access control list policer.	True	AVG
SUM_ACL_DISCARDED_PACKET_COUNT	COUNTER64	No	The sum of current number of discarded packets for the access control list policer.	True	SUM
AVG_ACL_ACCEPT_PACKET_COUNT	COUNTER64	No	The average of current number of discarded packets for the access control list policer.	True	AVG
SUM_ACL_ACCEPT_PACKET_COUNT	COUNTER64	No	The sum of current number of discarded packets for the access control list policer.	True	SUM
AVG_ACL_PEAK_DISCARD_RATE	GAUGE	No	The average of current peak discard rate for the access control list policer.	True	AVG
SUM_ACL_PEAK_DISCARD_RATE	GAUGE	No	The sum of current peak discard rate for the access control list policer.	True	SUM
AVG_ACL_MINOR_ALARM_COUNT	COUNTER	No	The average of current number of minor alarms for the access control list policer.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_ACL_MINOR_ALARM_COUNT	COUNTER	No	The sum of current number of minor alarms for the access control list policer.	True	SUM
AVG_ACL_MINOR_ALARM_DURATION	COUNTER	No	The average of current duration of the minor alarms in seconds for the access control list policer.	True	AVG
SUM_ACL_MINOR_ALARM_DURATION	COUNTER	No	The sum of current duration of the minor alarms in seconds for the access control list policer.	True	SUM
AVG_ACL_MAJOR_ALARM_COUNT	COUNTER	No	The average of current number of major alarms for the access control list policer.	True	AVG
SUM_ACL_MAJOR_ALARM_COUNT	COUNTER	No	The sum of current number of major alarms for the access control list policer.	True	SUM
AVG_ACL_MAJOR_ALARM_DURATION	COUNTER	No	The average of current duration of the major alarms in seconds for the access control list policer.	True	AVG
SUM_ACL_MAJOR_ALARM_DURATION	COUNTER	No	The sum of current duration of the major alarms in seconds for the access control list policer.	True	SUM
AVG_AGGREGATE_DISCARD_PKT_COUNT	COUNTER64	No	The average of current number of discarded packets for the aggregate policer.	True	AVG
SUM_AGGREGATE_DISCARD_PKT_COUNT	COUNTER64	No	The sum of current number of discarded packets for the aggregate policer.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_AGGREGATE_ACCEPT_PKT_COUNT	COUNTER64	No	The average of current number of discarded packets for the aggregate policer.	True	AVG
SUM_AGGREGATE_ACCEPT_PKT_COUNT	COUNTER64	No	The sum of current number of discarded packets for the aggregate policer.	True	SUM
AVG_AGGREGATE_PEAK_DISCARD_RATE	GAUGE	No	The average of current peak discard rate for the aggregate policer.	True	AVG
SUM_AGGREGATE_PEAK_DISCARD_RATE	GAUGE	No	The sum of current peak discard rate for the aggregate policer.	True	SUM
AVG_AGGREGATE_MINOR_ALARM_COUNT	COUNTER	No	The average of current number of minor alarms for the aggregate policer.	True	AVG
SUM_AGGREGATE_MINOR_ALARM_COUNT	COUNTER	No	The sum of current number of minor alarms for the aggregate policer.	True	SUM
AVG_AGGREGATE_MINOR_ALARM_DUR	COUNTER	No	The average of current duration of the minor alarms in seconds for the aggregate policer.	True	AVG
SUM_AGGREGATE_MINOR_ALARM_DUR	COUNTER	No	The sum of current duration of the minor alarms in seconds for the aggregate policer.	True	SUM
AVG_AGGREGATE_MAJOR_ALARM_COUNT	COUNTER	No	The average of current number of major alarms for the aggregate policer.	True	AVG
SUM_AGGREGATE_MAJOR_ALARM_COUNT	COUNTER	No	The sum of current number of major alarms for the aggregate policer.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_AGGREGATE_MAJOR_ALARM_DUR	COUNTER	No	The average of current duration of the major alarms in seconds for the aggregate policer.	True	AVG
SUM_AGGREGATE_MAJOR_ALARM_DUR	COUNTER	No	The sum of current duration of the major alarms in seconds for the aggregate policer.	True	SUM
AVG_MEDIA_DISCARD_PACKET_COUNT	COUNTER64	No	The average of current number of discarded packets for the media policer.	True	AVG
SUM_MEDIA_DISCARD_PACKET_COUNT	COUNTER64	No	The sum of current number of discarded packets for the media policer.	True	SUM
AVG_MEDIA_PEAK_DISCARD_RATE	GAUGE	No	The average of current peak discard rate for the media policer.	True	AVG
SUM_MEDIA_PEAK_DISCARD_RATE	GAUGE	No	The sum of current peak discard rate for the media policer.	True	SUM
AVG_MEDIA_MINOR_ALARM_COUNT	COUNTER	No	The average of current number of minor alarms for the media policer.	True	AVG
SUM_MEDIA_MINOR_ALARM_COUNT	COUNTER	No	The sum of current number of minor alarms for the media policer.	True	SUM
AVG_MEDIA_MINOR_ALARM_DURATION	COUNTER	No	The average of current duration of the minor alarms in seconds for the media policer.	True	AVG
SUM_MEDIA_MINOR_ALARM_DURATION	COUNTER	No	The sum of current duration of the minor alarms in seconds for the media policer.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_MEDIA_MAJOR_ALARM_COUNT	COUNTER	No	The average of current number of major alarms for the media policer.	True	AVG
SUM_MEDIA_MAJOR_ALARM_COUNT	COUNTER	No	The sum of current number of major alarms for the media policer.	True	SUM
AVG_MEDIA_MAJOR_ALARM_DURATION	COUNTER	No	The average of current duration of the major alarms in seconds for the media policer.	True	AVG
SUM_MEDIA_MAJOR_ALARM_DURATION	COUNTER	No	The sum of current duration of the major alarms in seconds for the media policer.		SUM
AVG_ROGUE_MEDIA_DISCARD_PACKET_COUNT	COUNTER64	No	The average of current number of discarded packets for the rogue media policer.	True	AVG
SUM_ROGUE_MEDIA_DISCARD_PACKET_COUNT	COUNTER64	No	The sum of current number of discarded packets for the rogue media policer.	True	SUM
AVG_ROGUE_MEDIA_PEAK_DISCARD_RATE	GAUGE	No	The average of current peak discard rate for the rogue media policer.	True	AVG
SUM_ROGUE_MEDIA_PEAK_DISCARD_RATE	GAUGE	No	The sum of current peak discard rate for the rogue media policer.	True	SUM
AVG_ROGUE_MEDIA_MINOR_ALARM_COUNT	COUNTER	No	The average of current number of minor alarms for the rogue media policer.	True	AVG
SUM_ROGUE_MEDIA_MINOR_ALARM_COUNT	COUNTER	No	The sum of current number of minor alarms for the rogue media policer.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_ROGUE_MEDIA_MINOR_ALARM_DUR	COUNTER	No	The average of current duration of the minor alarms in seconds for the rogue media policer.	True	AVG
SUM_ROGUE_MEDIA_MINOR_ALARM_DUR	COUNTER	No	The sum of current duration of the minor alarms in seconds for the rogue media policer.	True	SUM
AVG_ROGUE_MEDIA_MAJOR_ALARM_COUNT	COUNTER	No	The average of current number of major alarms for the rogue media policer.	True	AVG
SUM_ROGUE_MEDIA_MAJOR_ALARM_COUNT	COUNTER	No	The sum of current number of major alarms for the rogue media policer.	True	SUM
AVG_ROGUE_MEDIA_MAJOR_ALARM_DUR	COUNTER	No	The average of current duration of the major alarms in seconds for the rogue media policer.	True	AVG
SUM_ROGUE_MEDIA_MAJOR_ALARM_DUR	COUNTER	No	The sum of current duration of the major alarms in seconds for the rogue media policer.	True	SUM
AVG_DISCARD_RULE_PACKET_COUNT	COUNTER64	No	The average of current number of discarded packets for the IPSEC Decrypt policer.	True	AVG
SUM_DISCARD_RULE_PACKET_COUNT	COUNTER64	No	The sum of current number of discarded packets for the IPSEC Decrypt policer.	True	SUM
AVG_DISCARD_PEAK_DISCARD_RATE	GAUGE	No	The average of current peak discard rate for the discard rule.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_DISCARD_P EAK_DISCARD_R ATE	GAUGE	No	The sum of current peak discard rate for the discard rule.	True	SUM
AVG_DISCARD_MI NOR_ALARM_CO UNT	COUNTER	No	The average of current number of minor alarms for the discard rule.	True	AVG
SUM_DISCARD_M INOR_ALARM_CO UNT	COUNTER	No	The sum of current number of minor alarms for the discard rule.	True	SUM
AVG_DISCARD_MI NOR_ALARM_DU RATION	COUNTER	No	The average of current duration of the minor alarms in seconds for the discard rule.	True	AVG
SUM_DISCARD_M INOR_ALARM_DU RATION	COUNTER	No	The sum of current duration of the minor alarms in seconds for the discard rule.	True	SUM
AVG_DISCARD_M AJOR_ALARM_CO UNT	COUNTER	No	The average of current number of major alarms for the discard rule.	True	AVG
SUM_DISCARD_M AJOR_ALARM_CO UNT	COUNTER	No	The sum of current number of major alarms for the discard rule.	True	SUM
AVG_DISCARD_M AJOR_ALARM_DU RATION	COUNTER	No	The average of current duration of the major alarms in seconds for the discard rule.	True	AVG
SUM_DISCARD_M AJOR_ALARM_DU RATION	COUNTER	No	The sum of current duration of the major alarms in seconds for the discard rule.	True	SUM
AVG_DECRYPT_D ISCARD_PACKET_ COUNT	COUNTER	No	The average of count of packets discarded by SRTP decrypt discards.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_DECRYPT_DISCARD_PACKET_COUNT	COUNTER	No	The sum of count of packets discarded by SRTP decrypt discards.	True	SUM
AVG_PEAK_DECRYPT_DISCARD_RATE	COUNTER	No	The average of current peak discard rate for SRTP decrypt discards.	True	AVG
SUM_PEAK_DECRYPT_DISCARD_RATE	COUNTER	No	The sum of current peak discard rate for SRTP decrypt discards.	True	SUM
AVG_MINOR_DECRYPT_ALARM_COUNT	COUNTER	No	The average of current number of minor alarms for SRTP decrypt discards.	True	AVG
SUM_MINOR_DECRYPT_ALARM_COUNT	COUNTER	No	The sum of current number of minor alarms for SRTP decrypt discards.	True	SUM
AVG_MINOR_DECRYPT_ALARM_DURATION	COUNTER	No	The average of current duration of the minor alarms in seconds for SRTP decrypt discards.	True	AVG
SUM_MINOR_DECRYPT_ALARM_DURATION	COUNTER	No	The sum of current duration of the minor alarms in seconds for SRTP decrypt discards.	True	SUM
AVG_MAJOR_DECRYPT_ALARM_COUNT	COUNTER	No	The sum of current number of major alarms for the SRTP decrypt discards.	True	AVG
SUM_MAJOR_DECRYPT_ALARM_COUNT	COUNTER	No	The average of current number of major alarms for the SRTP decrypt discards.	True	SUM
AVG_MAJOR_DECRYPT_ALARM_DURATION	COUNTER	No	The sum of current duration of the major alarms in seconds for SRTP decrypt discards.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_MAJOR_DECRYPT_ALARM_DURATION	COUNTER	No	The average of current duration of the major alarms in seconds for SRTP decrypt discards.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

Link Stats

LinkDetectionGroupStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Link Detection Group - CLI
NAME	STRING	Yes	The link failure statistics per trunk group.	
SINGLE_FAILURES	INTEGER	No	The number of times a link monitor within this link detection group failed to receive a single echo reply. The first reattempt was successful.	
DOUBLE_FAILURES	INTEGER	No	The number of times a link monitor within this link detection group failed to receive two consecutive echo replies. The second (next) reattempt was successful.	
FAILURES	INTEGER	No	The number of times a link monitor within this link detection group declared itself failed.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

LinkMonitorStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Link Detection Group - CLI
GNAME	STRING	Yes	The name of the address context group.	
NAME	STRING	Yes	The name of the link monitor that monitors a link to a destination for a specific interface.	
MIN_TIME	INTEGER	No	The minimum time (in microseconds) used to get a reply for an echo request packet.	
MAX_TIME	INTEGER	No	The maximum time (in microseconds) used to get a reply for an echo request packet.	
AVERAGE_TIME	INTEGER	No	The average time (in microseconds) used to get a reply for an echo request packet.	
SINGLE_FAILURES	INTEGER	No	The number of single failures for this IP interface.	
DOUBLE_FAILURES	INTEGER	No	The number of double failures for this IP interface.	
FAILURES	INTEGER	No	The number of failures for this IP interface.	
REPLIES	INTEGER	No	The total number of replies.	
DUPLICATE_REPLIES	INTEGER	No	The number of duplicate replies.	
LATE_REPLIES	INTEGER	No	The number of late replies.	

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	No	The name of the compute element for this entry.	

NBS Stats

NBS5200CallCountStats

Column Name	Column Type	Index	Description	CLI Command Reference
KEY	IMPLIEDSTRING	Yes	Key value for the call.	Show Table System
CALL_ATTEMPTS	COUNTER	No	Number of call attempts on this server.	
CALL_COMPLETIONS	COUNTER	No	Total number of completed call attempts on this server.	
ACTIVE_CALLS	GAUGE	No	Current number of active managed calls on this server.	
STABLE_CALLS	GAUGE	No	Current number of stable managed calls on this server.	
MAX_LICENSE_LIMIT	INTEGER	No	This object indicates maximum license limit of this server.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

NBS5200CallCountStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
KEY	IMPLIEDSTRING	Yes	Key value for the call.	False	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
CALL_ATTEMPTS	COUNTER	No	Number of call attempts on this server.	True	SUM
CALL_COMPLETIONS	COUNTER	No	Total number of completed call attempts on this server.	True	SUM
ACTIVE_CALLS	GAUGE	No	Current number of active managed calls on this server.	False	MEAN
AVG_STABLE_CALLS	GAUGE	No	Current number of stable managed calls on this server.	False	MEAN
AVG_MAX_LICENSE_LIMIT	INTEGER	No	The average of maximum license limit of this server.	True	MEAN
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

NBS5200TGStatusStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of this Address Context.	False	N/A
ZNAME	STRING	Yes	The name of the address context zone.	False	N/A
NAME	STRING	Yes	The name of this IP trunk group.	False	N/A
AVG_STATE	INTEGER	No	The average of the current operational state of the IP trunk group.	True	AVG
AVG_TOTAL_CALLS_AVAILABLE	GAUGE	No	The average of the sum of all available or unblocked calls for this trunk group.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_TOTAL_CALLS_INBOUND_RESERVED	GAUGE	No	The average of the reserved count as specified by the percentage configured for this IP trunk group. This object shows the total number of calls that are reserved for inbound calls on this IP trunk group. This is applicable only for IP trunk groups that are configured for inbound or both directions.	True	AVG
AVG_INBOUND_CALLS_USAGE	GAUGE	No	The average of the current inbound or incoming usage count of this IP trunk group. This is applicable only for IP trunk groups that are configured for inbound or both directions.	True	AVG
AVG_OUTBOUND_CALLS_USAGE	GAUGE	No	The average of the current outbound, non-priority usage count of this IP trunk group.	True	AVG
AVG_TOTAL_CALLS_CONFIGURED	GAUGE	No	The average of the total number of calls that are configured on this IP trunk group.	True	AVG
AVG_TG_UTIL_PERCENT	INTEGER	No	This is calculated as: $\left(\frac{((\text{PSTN\_INBOUND\_USAGE} + \text{PSTN\_OUTBOUND\_USAGE}) * 100)}{\text{PSTN\_TOTAL\_CONFIGURED}} \right)$	True	AVG
AVG_PRIORITY_CALL_USAGE	GAUGE	No	The average of the current priority usage count of this IP trunk group. This is applicable for IP trunk groups that are configured with call reserved state enabled.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_TOTAL_OUTBOUND_CALLS_RESERVED	GAUGE	No	The average of the reserved count as specified by the percentage configured for this IP trunk group. This object reflects the total number of calls that are reserved for outbound calls on this IP trunk group. This is applicable for IP trunk groups that are configured for incoming call reservation.	True	AVG
AVG_BW_CURRENT_LIMIT	INTEGER	No	The average of the current bandwidth limit for this IP trunk group. It is initially set to the configured bandwidth limit but the packet outage detection events may reduce this limit.	True	AVG
AVG_BW_AVAILABLE	INTEGER	No	The average of the bandwidth available for allocation.	True	AVG
AVG_BW_INBOUND_USAGE	GAUGE	No	The average of the bandwidth in use for inbound traffic.	True	AVG
AVG_BW_OUTBOUND_USAGE	GAUGE	No	The average of the bandwidth in use for outbound traffic.	True	AVG
AVG_PACKET_OUT_DETECT_STATE	INTEGER	No	This average of the packet outage detection state. • normal - No packet outage is declared • packetOutageState - Packet outage is declared The packet outage detection bandwidth limit reduction reduces the current bandwidth limit.	True	AVG
AVG_PRIORITY_BW_USAGE	GAUGE	No	The average of the current media bandwidth in use for oversubscribed HPC/emergency calls (in Kbits/sec).	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

NBS5200TrunkGroupStatusStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of this Address Context.	Show Table System
ZNAME	STRING	Yes	The name of the address context zone.	
NAME	STRING	Yes	The name of this IP trunk group.	
STATE	INTEGER	No	Current operational state of the IP trunk group.	
TOTAL_CALLS_AVAILABLE	GAUGE	No	The sum of all available or unblocked calls for this trunk group.	
TOTAL_CALLS_INBOUND_RESERVED	GAUGE	No	The reserved count as specified by the percentage configured for this IP trunk group. This object shows the total number of calls that are reserved for inbound calls on this IP trunk group. This is applicable only for IP trunk groups that are configured for inbound or both directions.	
INBOUND_CALLS_USAGE	GAUGE	No	The current inbound or incoming usage count of this IP trunk group. This is applicable only for IP trunk groups that are configured for inbound or both directions.	

Column Name	Column Type	Index	Description	CLI Command Reference
OUTBOUND_CALLS_USAGE	GAUGE	No	The current outbound, non-priority usage count of this IP trunk group.	
TOTAL_CALLS_CONFIGURED	GAUGE	No	The total number of calls that are configured on this IP trunk group.	
TG_UTIL_PERCENT	INTEGER	No	This is calculated as: (((PSTN_INBOUND_USAGE + PSTN_OUTBOUND_USAGE) * 100) / PSTN_TOTAL_CONFIGURED)	
PRIORITY_CALL_USAGE	GAUGE	No	The current priority usage count of this IP trunk group. This is applicable for IP trunk groups that are configured with call reserved state enabled.	
TOTAL_OUTBOUND_CALLS_RESERVED	GAUGE	No	The reserved count as specified by the percentage configured for this IP trunk group. This object reflects the total number of calls that are reserved for outbound calls on this IP trunk group. This is applicable for IP trunk groups that are configured for incoming call reservation.	
BW_CURRENT_LIMIT	INTEGER	No	The current bandwidth limit for this IP trunk group. It is initially set to the configured bandwidth limit but the packet outage detection events may reduce the limit.	
BW_AVAILABLE	INTEGER	No	Bandwidth available for allocation.	

Column Name	Column Type	Index	Description	CLI Command Reference
BW_INBOUND_USAGE	GAUGE	No	Bandwidth in use for inbound traffic.	
BW_OUTBOUND_USAGE	GAUGE	No	Bandwidth in use for outbound traffic.	
PACKET_OUT_DETECT_STATE	INTEGER	No	This object indicates the packet outage detection state. - normal - No packet outage is declared - packetOutageState - Packet outage is declared The packet outage detection bandwidth limit reduction reduces the current bandwidth limit.	
PRIORITY_BW_USAGE	GAUGE	No	The current media bandwidth in use for oversubscribed HPC/emergency calls (in Kbits/sec).	
CE_NAME	STRING	No	The name of the compute element for this entry.	

RelayIntervalStatistics

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	true	The name of the address context.	false	N/A
KEY	COUNTER	False	Key value for the call.	false	N/A
NEW_CONN_CREATED	COUNTER	False	Total number of new relay connections created.	true	SUM
CONN_TERM_GRACEFULLY	COUNTER	False	The number of connections terminated gracefully.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
CONN_TERM_NO N_GRACEFULLY	COUNTER	True	The number of connections terminated non-gracefully.	true	SUM
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBCORE Stats

SBCCOREFacBlockingStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate type
KEY_TYPE	STRING	True	Key type such as call-id and calling party number.	False	N/A
KEY_ENTIT Y	STRING	True	Key values of call-id and calling party number.	False	N/A
BLOCK_CO UNT	INTEGER	False	The count of incoming packets dropped because of matching key/value pair of packet. The count is reset when a blocking entry is removed from the list. The entry is removed if the crash count is less than the configured threshold count or the entry is part of the facNonBlockingEntries list.	True	SUM
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBCCOREFacTotBlockStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate type
KEY_VAL	STRING	True	The dummy key for the list. At least one entry in the list is non-key.	False	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate type
TOTAL_BLOCK_COUNT	INTEGER	False	The count of packets dropped due to all blocking entries.	True	SUM
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBCCOREOodMessageIntStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
NAME	STRING	True	The name of this SIP IP Peer.	False	N/A
MESSAGE_RATE	COUNT	False	Number of incoming OOD requests received per second.	False	N/A
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBCCORESipIPResIntStat

Column name	Column type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	True	The name of this Address Context.	False	N/A
ZNAME	STRING	True	The name of the address context zone.	False	N/A
NAME	STRING	True	The name of this SIP IP Peer.	False	N/A
DIRECTION	STRING	True	The direction of (Interval) SIP response messages.	False	N/A
RESPONSE_CODE	INTEGER	True	The response code of (Interval) SIP response messages.	False	N/A

Column name	Column type	Index	Description	canAggregate	Aggregate Type
RESPONSE_COUNT	INTEGER	False	The total number of (Interval) SIP response messages for the specified response code.	True	AVG
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBCCORESipIPResIntStats_AG

Column name	Column type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	True	The name of this Address Context.	False	N/A
ZNAME	STRING	True	The name of the address context zone.	False	N/A
NAME	STRING	True	The name of this SIP IP Peer.	False	N/A
DIRECTION	STRING	True	The direction of (Interval) SIP response messages.	False	N/A
RESPONSE_CODE	INTEGER	True	The response code of (Interval) SIP response messages.	False	N/A
RESPONSE_COUNT	INTEGER	False	The total number of (Interval) SIP response messages for the specified response code.	True	AVG
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBCCORESipRegCountDomIntStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	true	The name of the address context.	false

Column Name	Column Type	Index	Description	canAggregate
DOMAIN_NAME	STRING	true	Domain name of the registration.	false
COUNT_ATTEMPTS	COUNTER	true	The number of SIP registration attempts.	false
COUNTCUM_COMPLETED	COUNTER	false	The accumulative number of completed SIP registration attempts.	true
COUNT_PENDING	COUNTER	false	The current number of pending SIP registrations.	true
COUNT_STABLE	COUNTER	false	The current number of stable SIP registrations.	true
COUNT_TOTAL	COUNTER	false	The total number of current SIP registrations.	true
EMERGENCY_ACC_TOT	COUNTER	false	The total number of accepted emergency SIP registrations.	true
EMERGENCY_COUNT_ACT	COUNTER	false	The total number of active emergency SIP registrations.	true
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SBCCORESipRegCountDomIntStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
ACNAME	STRING	true	The name of the address context.	false	N/A
DOMAIN_NAME	STRING	true	Domain name of the registration.	false	N/A
COUNT_ATTEMPTS	COUNTER	true	The number of SIP registration attempts.	false	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_COUNTCUM_COMPLETED	COUNTER	false	The accumulative number of completed SIP registration attempts.	true	SUM
SUM_COUNT_PENDING	COUNTER	false	The current number of pending SIP registrations.	true	SUM
SUM_COUNT_STABLE	COUNTER	false	The current number of stable SIP registrations.	true	SUM
SUM_COUNT_TOTAL	COUNTER	false	The total number of current SIP registrations.	true	SUM
SUM_EMERGENCY_ACC_TOT	COUNTER	false	The total number of accepted emergency SIP registrations.	true	SUM
SUM_EMERGENCY_COUNT_ACT	COUNTER	false	The total number of active emergency SIP registrations.	true	SUM
CE_NAME	STRING	false	The name of the compute element for this entry.	false	N/A

SBCCORESipTGAggregatedStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
DIRECTION	STRING	True	The direction of SIP call.	False	N/A
RESPONSE_CODE	INTEGER	True	The response code of SIP call.	False	N/A
RESPONSE_COUNT	COUNTER	True	The total number of SIP responses.	True	SUM
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBCCORESipTgCSSRIntStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	true	The name of the address context.	false
ZNAME	STRING	true	The name of the address context zone.	false
NAME	STRING	true	The name of this SIP trunk group.	false
INV_SENT	COUNTER	false	The total number of (interval) inv_sent.	true
INV_RCVD	COUNTER	false	The total number of (interval) inv_rcvd.	true
ALERT_SENT	COUNTER	false	The total number of (interval) 18x_sent.	true
ALERT_RCVD	COUNTER	false	The total number of (interval) 18x_rcvd.	true
ANSCALLS_SENT	COUNTER	false	The total number of (interval) ansCalls_sent.	true
ANSCALLS_RCVD	COUNTER	false	The total number of (interval) ansCalls_rcvd.	true
CANCEL_SENT	COUNTER	false	The total number of (interval) cancel_sent.	true
CANCEL_RCVD	COUNTER	false	The total number of (interval) cancel_rcvd.	true
BYE_SENT	COUNTER	false	The total number of (interval) bye_sent.	true
BYE_RCVD	COUNTER	false	The total number of (interval) bye_rcvd.	true
INV200_SENT	COUNTER	false	The total number of (interval) inv200_sent.	true

Column Name	Column Type	Index	Description	canAggregate
INV200_RCVD	COUNTER	false	The total number of (interval) inv200_sent.	true
INV380_SENT	COUNTER	false	The total number of (interval) inv380_sent.	true
INV380_RCVD	COUNTER	false	The total number of (interval) inv380_rcvd.	true
INV400_SENT	COUNTER	false	The total number of (interval) inv400_sent.	true
INV400_RCVD	COUNTER	false	The total number of (interval) inv400_rcvd.	true
INV403_SENT	COUNTER	false	The total number of (interval) inv403_sent.	true
INV403_RCVD	COUNTER	false	The total number of (interval) inv403_rcvd.	true
INV404_SENT	COUNTER	false	The total number of (interval) inv404_sent.	true
INV404_RCVD	COUNTER	false	The total number of (interval) inv404_rcvd.	true
INV406_SENT	COUNTER	false	The total number of (interval) inv406_sent.	true
INV406_RCVD	COUNTER	false	The total number of (interval) inv406_rcvd.	true
INV408_SENT	COUNTER	false	The total number of (interval) inv408_sent.	true
INV408_RCVD	COUNTER	false	The total number of (interval) inv408_rcvd.	true
INV410_SENT	COUNTER	false	The total number of (interval) inv410_sent.	true
INV410_RCVD	COUNTER	false	The total number of (interval) inv410_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
INV420_SENT	COUNTER	false	The total number of (interval) inv420_sent.	true
INV420_RCVD	COUNTER	false	The total number of (interval) inv420_rcvd.	true
INV480_SENT	COUNTER	false	The total number of (interval) inv480_sent.	true
INV480_RCVD	COUNTER	false	The total number of (interval) inv480_rcvd.	true
INV481_SENT	COUNTER	false	The total number of (interval) inv481_sent.	true
INV481_RCVD	COUNTER	false	The total number of (interval) inv481_rcvd.	true
INV482_SENT	COUNTER	false	The total number of (interval) inv482_sent.	true
INV482_RCVD	COUNTER	false	The total number of (interval) inv482_rcvd.	true
INV483_SENT	COUNTER	false	The total number of (interval) inv483_sent.	true
INV483_RCVD	COUNTER	false	The total number of (interval) inv483_rcvd.	true
INV484_SENT	COUNTER	false	The total number of (interval) inv484_sent.	true
INV484_RCVD	COUNTER	false	The total number of (interval) inv484_rcvd.	true
INV486_SENT	COUNTER	false	The total number of (interval) inv486_sent.	true
INV486_RCVD	COUNTER	false	The total number of (interval) inv486_rcvd.	true
INV487_SENT	COUNTER	false	The total number of (interval) inv487_sent.	true

Column Name	Column Type	Index	Description	canAggregate
INV487_RCVD	COUNTER	false	The total number of (interval) inv487_rcvd.	true
INV488_SENT	COUNTER	false	The total number of (interval) inv488_sent.	true
INV488_RCVD	COUNTER	false	The total number of (interval) inv488_rcvd.	true
INV500_SENT	COUNTER	false	The total number of (interval) inv500_sent.	true
INV500_RCVD	COUNTER	false	The total number of (interval) inv500_rcvd.	true
INV501_SENT	COUNTER	false	The total number of (interval) inv501_sent.	true
INV501_RCVD	COUNTER	false	The total number of (interval) inv501_rcvd.	true
INV502_SENT	COUNTER	false	The total number of (interval) inv502_sent.	true
INV502_RCVD	COUNTER	false	The total number of (interval) inv502_rcvd.	true
INV503_SENT	COUNTER	false	The total number of (interval) inv503_sent.	true
INV503_RCVD	COUNTER	false	The total number of (interval) inv503_rcvd.	true
INV504_SENT	COUNTER	false	The total number of (interval) inv504_sent.	true
INV504_RCVD	COUNTER	false	The total number of (interval) inv504_rcvd.	true
INV580_SENT	COUNTER	false	The total number of (interval) inv580_sent.	true
INV580_RCVD	COUNTER	false	The total number of (interval) inv580_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
INV602_SENT	COUNTER	false	The total number of (interval) inv602_sent.	true
INV602_RCVD	COUNTER	false	The total number of (interval) inv602_rcvd.	true
INV603_SENT	COUNTER	false	The total number of (interval) inv603_sent.	true
INV603_RCVD	COUNTER	false	The total number of (interval) inv603_rcvd.	true
INV606_SENT	COUNTER	false	The total number of (interval) inv606_sent.	true
INV606_RCVD	COUNTER	false	The total number of (interval) inv606_rcvd.	true
INVUNKNOWN_SENT	COUNTER	false	The total number of (interval) invUnknown_sent.	true
INVUNKNOWN_RCVD	COUNTER	false	The total number of (interval) invUnknown_rcvd.	true
NON_INV200_SENT	COUNTER	false	The total number of (interval) nonInv200_sent.	true
NON_INV200_RCVD	COUNTER	false	The total number of (interval) nonInv200_rcvd.	true
NON_INV380_SENT	COUNTER	false	The total number of (interval) nonInv380_sent.	true
NON_INV380_RCVD	COUNTER	false	The total number of (interval) nonInv380_rcvd.	true
NON_INV400_SENT	COUNTER	false	The total number of (interval) nonInv400_sent.	true
NON_INV400_RCVD	COUNTER	false	The total number of (interval) nonInv400_rcvd.	true
NON_INV403_SENT	COUNTER	false	The total number of (interval) nonInv403_sent.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INV403_RCVD	COUNTER	false	The total number of (interval) nonInv403_rcvd.	true
NON_INV404_SENT	COUNTER	false	The total number of (interval) nonInv404_sent.	true
NON_INV404_RCVD	COUNTER	false	The total number of (interval) nonInv404_rcvd.	true
NON_INV406_SENT	COUNTER	false	The total number of (interval) nonInv406_sent.	true
NON_INV406_RCVD	COUNTER	false	The total number of (interval) nonInv406_rcvd.	true
NON_INV408_SENT	COUNTER	false	The total number of (interval) nonInv408_sent.	true
NON_INV408_RCVD	COUNTER	false	The total number of (interval) nonInv408_rcvd.	true
NON_INV410_SENT	COUNTER	false	The total number of (interval) nonInv410_sent.	true
NON_INV410_RCVD	COUNTER	false	The total number of (interval) nonInv410_rcvd.	true
NON_INV420_SENT	COUNTER	false	The total number of (interval) nonInv420_sent.	true
NON_INV420_RCVD	COUNTER	false	The total number of (interval) nonInv420_rcvd.	true
NON_INV480_SENT	COUNTER	false	The total number of (interval) nonInv480_sent.	true
NON_INV480_RCVD	COUNTER	false	The total number of (interval) nonInv480_rcvd.	true
NON_INV481_SENT	COUNTER	false	The total number of (interval) nonInv481_sent.	true
NON_INV481_RCVD	COUNTER	false	The total number of (interval) nonInv481_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INV482_SENT	COUNTER	false	The total number of (interval) nonInv482_sent.	true
NON_INV482_RCVD	COUNTER	false	The total number of (interval) nonInv482_rcvd.	true
NON_INV483_SENT	COUNTER	false	The total number of (interval) nonInv483_sent.	true
NON_INV483_RCVD	COUNTER	false	The total number of (interval) nonInv483_rcvd.	true
NON_INV484_SENT	COUNTER	false	The total number of (interval) nonInv484_sent.	true
NON_INV484_RCVD	COUNTER	false	The total number of (interval) nonInv484_rcvd.	true
NON_INV486_SENT	COUNTER	false	The total number of (interval) nonInv486_sent.	true
NON_INV486_RCVD	COUNTER	false	The total number of (interval) nonInv486_rcvd.	true
NON_INV487_SENT	COUNTER	false	The total number of (interval) nonInv487_sent.	true
NON_INV487_RCVD	COUNTER	false	The total number of (interval) nonInv487_rcvd.	true
NON_INV488_SENT	COUNTER	false	The total number of (interval) nonInv488_sent.	true
NON_INV488_RCVD	COUNTER	false	The total number of (interval) nonInv488_rcvd.	true
NON_INV500_SENT	COUNTER	false	The total number of (interval) nonInv500_sent.	true
NON_INV500_RCVD	COUNTER	false	The total number of (interval) nonInv500_rcvd.	true
NON_INV501_SENT	COUNTER	false	The total number of (interval) nonInv501_sent.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INV501_RCVD	COUNTER	false	The total number of (interval) nonInv501_rcvd.	true
NON_INV502_SENT	COUNTER	false	The total number of (interval) nonInv502_sent.	true
NON_INV502_RCVD	COUNTER	false	The total number of (interval) nonInv502_rcvd.	true
NON_INV503_SENT	COUNTER	false	The total number of (interval) nonInv503_sent.	true
NON_INV503_RCVD	COUNTER	false	The total number of (interval) nonInv503_rcvd.	true
NON_INV504_SENT	COUNTER	false	The total number of (interval) nonInv504_sent.	true
NON_INV504_RCVD	COUNTER	false	The total number of (interval) nonInv504_rcvd.	true
NON_INV580_SENT	COUNTER	false	The total number of (interval) nonInv580_sent.	true
NON_INV580_RCVD	COUNTER	false	The total number of (interval) nonInv580_rcvd.	true
NON_INV602_SENT	COUNTER	false	The total number of (interval) nonInv602_sent.	true
NON_INV602_RCVD	COUNTER	false	The total number of (interval) nonInv602_rcvd.	true
NON_INV603_SENT	COUNTER	false	The total number of (interval) nonInv603_sent.	true
NON_INV603_RCVD	COUNTER	false	The total number of (interval) nonInv603_rcvd.	true
NON_INV606_SENT	COUNTER	false	The total number of (interval) nonInv606_sent.	true
INV606_RCVD	COUNTER	false	The total number of (interval) nonInv606_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INVUNKNOWN_SENT	COUNTER	false	The total number of (interval) nonInvUnknown_sent.	true
NON_INVUNKNOWN_RCVD	COUNTER	false	The total number of (interval) nonInvUnknown_rcvd.	true
CE_NAME	STRING	false	The name of the compute element for this entry.	False

SBCCORESipTgCSSRIntStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
ACNAME	STRING	true	The name of the address context.	false	N/A
ZNAME	STRING	true	The name of the address context zone.	false	N/A
NAME	STRING	true	The name of this SIP trunk group.	false	N/A
SUM_INV_SENT	COUNTER	false	The total number of (interval) inv_sent.	true	SUM
SUM_INV_RCVD	COUNTER	false	The total number of (interval) inv_rcvd.	true	SUM
SUM_ALERT_SENT	COUNTER	false	The total number of (interval) 18x_sent.	true	SUM
SUM_ALERT_RCVD	COUNTER	false	The total number of (interval) 18x_rcvd.	true	SUM
SUM_ANSCALLS_SENT	COUNTER	false	The total number of (interval) ansCalls_sent.	true	SUM
SUM_ANSCALLS_RCVD	COUNTER	false	The total number of (interval) ansCalls_rcvd.	true	SUM
SUM_CANCEL_SENT	COUNTER	false	The total number of (interval) cancel_sent.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_CANCEL_R CVD	COUNTER	false	The total number of (interval) cancel_rcvd.	true	SUM
SUM_BYE_SENT	COUNTER	false	The total number of (interval) bye_sent.	true	SUM
SUM_BYE_RCVD	COUNTER	false	The total number of (interval) bye_rcvd.	true	SUM
SUM_INV200_SE NT	COUNTER	false	The total number of (interval) inv200_sent.	true	SUM
SUM_INV200_RC VD	COUNTER	false	The total number of (interval) inv200_rcvd.	true	SUM
SUM_INV380_SE NT	COUNTER	false	The total number of (interval) inv380_sent.	true	SUM
SUM_INV380_RC VD	COUNTER	false	The total number of (interval) inv380_rcvd.	true	SUM
SUM_INV400_SE NT	COUNTER	false	The total number of (interval) inv400_sent.	true	SUM
SUM_INV400_RC VD	COUNTER	false	The total number of (interval) inv400_rcvd.	true	SUM
SUM_INV403_SE NT	COUNTER	false	The total number of (interval) inv403_sent.	true	SUM
SUM_INV403_RC VD	COUNTER	false	The total number of (interval) inv403_rcvd.	true	SUM
SUM_INV404_SE NT	COUNTER	false	The total number of (interval) inv404_sent.	true	SUM
SUM_INV404_RC VD	COUNTER	false	The total number of (interval) inv404_rcvd.	true	SUM
SUM_INV406_SE NT	COUNTER	false	The total number of (interval) inv406_sent.	true	SUM
SUM_INV406_RC VD	COUNTER	false	The total number of (interval) inv406_rcvd.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_INV408_SENT	COUNTER	false	The total number of (interval) inv408_sent.	true	SUM
SUM_INV408_RCVD	COUNTER	false	The total number of (interval) inv408_rcvd.	true	SUM
SUM_INV410_SENT	COUNTER	false	The total number of (interval) inv410_sent.	true	SUM
SUM_INV410_RCVD	COUNTER	false	The total number of (interval) inv410_rcvd.	true	SUM
SUM_INV420_SENT	COUNTER	false	The total number of (interval) inv420_sent.	true	SUM
SUM_INV420_RCVD	COUNTER	false	The total number of (interval) inv420_rcvd.	true	SUM
SUM_INV480_SENT	COUNTER	false	The total number of (interval) inv480_sent.	true	SUM
SUM_INV480_RCVD	COUNTER	false	The total number of (interval) inv480_rcvd.	true	SUM
SUM_INV481_SENT	COUNTER	false	The total number of (interval) inv481_sent.	true	SUM
SUM_INV481_RCVD	COUNTER	false	The total number of (interval) inv481_rcvd.	true	SUM
SUM_INV482_SENT	COUNTER	false	The total number of (interval) inv482_sent.	true	SUM
SUM_INV482_RCVD	COUNTER	false	The total number of (interval) inv482_rcvd.	true	SUM
SUM_INV483_SENT	COUNTER	false	The total number of (interval) inv483_sent.	true	SUM
SUM_INV483_RCVD	COUNTER	false	The total number of (interval) inv483_rcvd.	true	SUM
SUM_INV484_SENT	COUNTER	false	The total number of (interval) inv484_sent.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_INV484_RC VD	COUNTER	false	The total number of (interval) inv484_rcvd.	true	SUM
SUM_INV486_SE NT	COUNTER	false	The total number of (interval) inv486_sent.	true	SUM
SUM_INV486_RC VD	COUNTER	false	The total number of (interval) inv486_rcvd.	true	SUM
SUM_INV487_SE NT	COUNTER	false	The total number of (interval) inv487_sent.	true	SUM
SUM_INV487_RC VD	COUNTER	false	The total number of (interval) inv487_rcvd.	true	SUM
SUM_INV488_SE NT	COUNTER	false	The total number of (interval) inv488_sent.	true	SUM
SUM_INV488_RC VD	COUNTER	false	The total number of (interval) inv488_rcvd.	true	SUM
SUM_INV500_SE NT	COUNTER	false	The total number of (interval) inv500_sent.	true	SUM
SUM_INV500_RC VD	COUNTER	false	The total number of (interval) inv500_rcvd.	true	SUM
SUM_INV501_SE NT	COUNTER	false	The total number of (interval) inv501_sent.	true	SUM
SUM_INV501_RC VD	COUNTER	false	The total number of (interval) inv501_rcvd.	true	SUM
SUM_INV502_SE NT	COUNTER	false	The total number of (interval) inv502_sent.	true	SUM
SUM_INV502_RC VD	COUNTER	false	The total number of (interval) inv502_rcvd.	true	SUM
SUM_INV503_SE NT	COUNTER	false	The total number of (interval) inv503_sent.	true	SUM
SUM_INV503_RC VD	COUNTER	false	The total number of (interval) inv503_rcvd.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_INV504_SENT	COUNTER	false	The total number of (interval) inv504_sent.	true	SUM
SUM_INV504_RCVD	COUNTER	false	The total number of (interval) inv504_rcvd.	true	SUM
SUM_INV580_SENT	COUNTER	false	The total number of (interval) inv580_sent.	true	SUM
SUM_INV580_RCVD	COUNTER	false	The total number of (interval) inv580_rcvd.	true	SUM
SUM_INV602_SENT	COUNTER	false	The total number of (interval) inv602_sent.	true	SUM
SUM_INV602_RCVD	COUNTER	false	The total number of (interval) inv602_rcvd.	true	SUM
SUM_INV603_SENT	COUNTER	false	The total number of (interval) inv603_sent.	true	SUM
SUM_INV603_RCVD	COUNTER	false	The total number of (interval) inv603_rcvd.	true	SUM
SUM_INV606_SENT	COUNTER	false	The total number of (interval) inv606_sent.	true	SUM
SUM_INV606_RCVD	COUNTER	false	The total number of (interval) inv606_rcvd.	true	SUM
SUM_INVUNKNO WN_SENT	COUNTER	false	The total number of (interval) invUnknown_sent.	true	SUM
SUM_INVUNKNO WN_RCVD	COUNTER	false	The total number of (interval) invUnknown_rcvd.	true	SUM
SUM_NON_INV200_SENT	COUNTER	false	The total number of (interval) nonInv200_sent.	true	SUM
SUM_NON_INV200_RCVD	COUNTER	false	The total number of (interval) nonInv200_sent.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_NON_INV380_SENT	COUNTER	false	The total number of (interval) nonInv380_sent.	true	SUM
SUM_NON_INV380_RCVD	COUNTER	false	The total number of (interval) nonInv380_rcvd.	true	SUM
SUM_NON_INV400_SENT	COUNTER	false	The total number of (interval) nonInv400_sent.	true	SUM
SUM_NON_INV400_RCVD	COUNTER	false	The total number of (interval) nonInv400_rcvd.	true	SUM
SUM_NON_INV403_SENT	COUNTER	false	The total number of (interval) nonInv403_sent.	true	SUM
SUM_NON_INV403_RCVD	COUNTER	false	The total number of (interval) nonInv403_rcvd.	true	SUM
SUM_NON_INV404_SENT	COUNTER	false	The total number of (interval) nonInv404_sent.	true	SUM
SUM_NON_INV404_RCVD	COUNTER	false	The total number of (interval) nonInv404_rcvd.	true	SUM
SUM_NON_INV406_SENT	COUNTER	false	The total number of (interval) nonInv406_sent.	true	SUM
SUM_NON_INV406_RCVD	COUNTER	false	The total number of (interval) nonInv406_rcvd.	true	SUM
SUM_NON_INV408_SENT	COUNTER	false	The total number of (interval) nonInv408_sent.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_NON_INV408_RCVD	COUNTER	false	The total number of (interval) nonInv408_rcvd.	true	SUM
SUM_NON_INV410_SENT	COUNTER	false	The total number of (interval) nonInv410_sent.	true	SUM
SUM_NON_INV410_RCVD	COUNTER	false	The total number of (interval) nonInv410_rcvd.	true	SUM
SUM_NON_INV420_SENT	COUNTER	false	The total number of (interval) nonInv420_sent.	true	SUM
SUM_NON_INV420_RCVD	COUNTER	false	The total number of (interval) nonInv420_rcvd.	true	SUM
SUM_NON_INV480_SENT	COUNTER	false	The total number of (interval) nonInv480_sent.	true	SUM
SUM_NON_INV480_RCVD	COUNTER	false	The total number of (interval) nonInv480_rcvd.	true	SUM
SUM_NON_INV481_SENT	COUNTER	false	The total number of (interval) nonInv481_sent.	true	SUM
SUM_NON_INV481_RCVD	COUNTER	false	The total number of (interval) nonInv481_rcvd.	true	SUM
SUM_NON_INV482_SENT	COUNTER	false	The total number of (interval) nonInv482_sent.	true	SUM
SUM_NON_INV482_RCVD	COUNTER	false	The total number of (interval) nonInv482_rcvd.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_NON_INV48 3_SENT	COUNTER	false	The total number of (interval) nonInv483_sent.	true	SUM
SUM_NON_INV48 3_RCVD	COUNTER	false	The total number of (interval) nonInv483_rcvd.	true	SUM
SUM_NON_INV48 4_SENT	COUNTER	false	The total number of (interval) nonInv484_sent.	true	SUM
SUM_NON_INV48 4_RCVD	COUNTER	false	The total number of (interval) nonInv484_rcvd.	true	SUM
SUM_NON_INV48 6_SENT	COUNTER	false	The total number of (interval) nonInv486_sent.	true	SUM
SUM_NON_INV48 6_RCVD	COUNTER	false	The total number of (interval) nonInv486_rcvd.	true	SUM
SUM_NON_INV48 7_SENT	COUNTER	false	The total number of (interval) nonInv487_sent.	true	SUM
SUM_NON_INV48 7_RCVD	COUNTER	false	The total number of (interval) nonInv487_rcvd.	true	SUM
SUM_NON_INV48 8_SENT	COUNTER	false	The total number of (interval) nonInv488_sent.	true	SUM
SUM_NON_INV48 8_RCVD	COUNTER	false	The total number of (interval) nonInv488_rcvd.	true	SUM
SUM_NON_INV50 0_SENT	COUNTER	false	The total number of (interval) nonInv500_sent.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_NON_INV500_RCVD	COUNTER	false	The total number of (interval) nonInv500_rcvd.	true	SUM
SUM_NON_INV501_SENT	COUNTER	false	The total number of (interval) nonInv501_sent.	true	SUM
SUM_NON_INV501_RCVD	COUNTER	false	The total number of (interval) nonInv501_rcvd.	true	SUM
SUM_NON_INV502_SENT	COUNTER	false	The total number of (interval) nonInv502_sent.	true	SUM
SUM_NON_INV502_RCVD	COUNTER	false	The total number of (interval) nonInv502_rcvd.	true	SUM
SUM_NON_INV503_SENT	COUNTER	false	The total number of (interval) nonInv503_sent.	true	SUM
SUM_NON_INV503_RCVD	COUNTER	false	The total number of (interval) nonInv503_rcvd.	true	SUM
SUM_NON_INV504_SENT	COUNTER	false	The total number of (interval) nonInv504_sent.	true	SUM
SUM_NON_INV504_RCVD	COUNTER	false	The total number of (interval) nonInv504_rcvd.	true	SUM
SUM_NON_INV580_SENT	COUNTER	false	The total number of (interval) nonInv580_sent.	true	SUM
SUM_NON_INV580_RCVD	COUNTER	false	The total number of (interval) nonInv580_rcvd.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_NON_INV602_SENT	COUNTER	false	The total number of (interval) nonInv602_sent.	true	SUM
SUM_NON_INV602_RCVD	COUNTER	false	The total number of (interval) nonInv602_rcvd.	true	SUM
SUM_NON_INV603_SENT	COUNTER	false	The total number of (interval) nonInv603_sent.	true	SUM
SUM_NON_INV603_RCVD	COUNTER	false	The total number of (interval) nonInv603_rcvd.	true	SUM
SUM_SUM_NON_INV606_SENT	COUNTER	false	The total number of (interval) nonInv606_sent.	true	SUM
SUM_INV606_RCVD	COUNTER	false	The total number of (interval) nonInv606_rcvd.	true	SUM
SUM_NON_INVU_NKNOWN_SENT	COUNTER	false	The total number of (interval) nonInvUnknown_sent.	true	SUM
SUM_NON_INVU_NKNOWN_RCVD	COUNTER	false	The total number of (interval) nonInvUnknown_rcvd.	true	SUM
CE_NAME	STRING	false	The name of the compute element for this entry.	false	N/A

SBCCORESipTGResIntStats

Column name	Column type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	True	The name of this address context.	False	N/A
ZNAME	STRING	True	The name of the address context zone.	False	N/A

Column name	Column type	Index	Description	canAggregate	Aggregate Type
NAME	STRING	True	The name of this SIP trunk group.	False	N/A
DIRECTION	STRING	True	The direction of (Interval) SIP response messages.	False	N/A
RESPONSE_CODE	INTEGER	True	The response code of (Interval) SIP response messages.	False	N/A
RESPONSE_COUNT	INTEGER	False	The total number of (Interval) SIP response messages for the specified response code.	True	AVG
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBCCORESipTGResIntStats_AG

Column name	Column type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	True	The name of this Address Context.	False	N/A
ZNAME	STRING	True	The name of the address context zone.	False	N/A
NAME	STRING	True	The name of this SIP trunk group.	False	N/A
DIRECTION	STRING	True	The direction of (Interval) SIP response messages.	False	N/A
RESPONSE_CODE	INTEGER	True	The response code of (Interval) SIP response messages.	False	N/A
RESPONSE_COUNT	INTEGER	False	The total number of (Interval) SIP response messages for the specified response code.	True	AVG

Column name	Column type	Index	Description	canAggregate	Aggregate Type
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBCCORETGAggregatedStats

Column Name	Column Type	Index	canAggregate
DIRECTION	STRING	True	False
RESCODE	INTEGER	True	False
RESCOUNT	COUNTER	True	True
CE_NAME	STRING	No	False

SBX5K Stats

SBX5KAclOffListIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

SBX5KAggregateOffIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

SBX5KArpOffListIntStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	N/A	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	AVG	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	N/A	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	N/A	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	N/A	

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	CLI Command Reference
SOURCE_IP_ADDRESS	STRING	No	The source IP port of the table entry.	True	N/A	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	N/A	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	AVG	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A	

SBX5KBadEtherIpHdrOffIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
ETHER_TYPE	INTEGER	No	The first ether type found in the Ethernet packet.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

SBX5KDiscardRuleOffIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

SBX5KDtlsSrtpStats

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	The name of the compute element for this entry.	DTLS Profile - CLI
CURRENT_CLIENT_CONNECTIONS	INTEGER	No	Number of client sessions currently active.	
CURRENT_SERVER_CONNECTIONS	INTEGER	No	Number of server sessions currently active.	
TOTAL_CLIENT_SESSIONS	INTEGER	No	Cumulative total number of client sessions.	
TOTAL_SERVER_SESSIONS	INTEGER	No	Cumulative total number of server sessions.	

Column Name	Column Type	Index	Description	CLI Command Reference
SUCCESSFUL_CLIENT_HANDSHAKES	INTEGER	No	Number of successful client handshakes.	
SUCCESSFUL_SERVER_HANDSHAKES	INTEGER	No	Number of successful server handshakes.	
SESSION_RESUMPTIONS	INTEGER	No	Number of server sessions that resume.	
NO_CIPHER_SUITE	INTEGER	No	Number of handshake failures due to inability to converge on a cipher suite.	
HANDSHAKE_TIMEOUTS	INTEGER	No	Number of handshakes that timed out before completing.	
CLIENT_AUTH_FAILURES	INTEGER	No	Number of times peer failed DTLS authentication with SBC as the client.	
SERVER_AUTH_FAILURES	INTEGER	No	Number of times peer failed DTLS authentication with SBC as the server.	
FATAL_ALERTS_RECEIVED	INTEGER	No	Number of FATAL Alerts received.	
WARNING_ALERTS_RECEIVED	INTEGER	No	Number of WARNING Alerts received.	
HANDSHAKE_FAILURES	INTEGER	No	Cumulative total of all handshake failures.	
RECEIVE_FAILURES	INTEGER	No	Number of receive failures (failure to decrypt).	
SEND_FAILURES	INTEGER	No	Number of send failures (failure to encrypt).	
NO_CLIENT_CERT	INTEGER	No	Number times we were the client and we failed to derive a certificate to send the server.	

Column Name	Column Type	Index	Description	CLI Command Reference
VERSION_MISMATCH	INTEGER	No	Number of failed version MisMatch.	
FINGERPRINT_MISMATCH	INTEGER	No	FingerPrint MisMatch	
NO_SRTP_PROFILE	INTEGER	No	No Srtp Profile.	

SBX5KEthernetPortPacketPortStatus

Column Name	Column Type	Index	Description	CLI Command Reference
AVG_RX_ACTUAL_BW	Gauge	False	Tracks the Average Incoming Bandwidth used during KPI bin interval in bytes/sec.	Master Trunk Group - CLI (Show Table Address Context - IP Interface Group)
AVG_TX_ACTUAL_BW	Gauge	False	Tracks the Average Outgoing Bandwidth used during KPI bin interval in bytes/sec.	
PEAK_RX_ACTUAL_BW	Gauge	False	Tracks the Peak Incoming Bandwidth used during KPI bin interval in bytes/sec.	
PEAK_TX_ACTUAL_BW	Gauge	False	Tracks the Peak Outgoing Bandwidth used during KPI bin interval in bytes/sec.	
AVG_RX_ACTUAL_BWUTIL	Gauge	False	Tracks the average incoming BW utilization based on total available port BW instead of negotiated BW.	
PEAK_RX_ACTUAL_BWUTIL	Gauge	False	Tracks the maximum incoming BW utilization during the KPI bin interval expressed as a percentage of the available BW.	
AVG_TX_ACTUAL_BWUTIL	Gauge	False	Tracks the average outgoing BW utilization during the KPI bin interval based on total available BW instead of negotiated BW.	
PEAK_TX_ACTUAL_BWUTIL	Gauge	False	Tracks the maximum outgoing BW utilization during the KPI bin interval expressed as a percentage of the available BW.	
BWALARM_THRESHOLD_EXCEEDED	Gauge	False	Tracks the total number of times the BW alarm threshold was passed in the upward direction during the bin interval	

Column Name	Column Type	Index	Description	CLI Command Reference
BWALARM_CLEARED	GAUGE	False	Tracks the total number of times the BW clear alarm threshold was passed in the downward direction during the bin interval.	
AVG_USAGE_BW	GAUGE	False	Tracks the Average Bandwidth Usage during KPI bin interval	
PEAK_USAGE_BW	GAUGE	False	Tracks the Peak Bandwidth Usage during KPI bin interval.	
CE_NAME	STRING	True	The host name of the server.	
PORT_NAME	STRING	True	The name of this port.	
NEGOTIATED_SPEED	INTEGER	False	The interface speed. Packet port speed is not negotiable.	
LINK_STATE	INTEGER	False	The state of the interface.	
MAX_BANDWIDTH	GAUGE	False	Maximum bandwidth this port can support, bytes/sec.	
ALLOCATED_BANDWIDTH	GAUGE	False	Bandwidth the active media streams on this port reserve, bytes/sec.	
RX_BANDWIDTH	GAUGE	False	Actual Rx bandwidth in use on this port, bytes/sec.	
TX_BANDWIDTH	GAUGE	False	Actual Tx bandwidth in use on this port, bytes/sec.	
BANDWIDTH_USAGE	GAUGE	False	Percentage of maximum bandwidth allocated on this port.	
BANDWIDTH_DEVIATION	GAUGE	False	Percentage of deviation of actual bandwidth from the allocated bandwidth.	
MAC_ADDRESS	STRING	False	The MAC address of the network interface.	

Column Name	Column Type	Index	Description	CLI Command Reference
IF_INDEX	GAUGE	False	The unique ifIndex of this Packet NIF.	

SBX5KIpSecDecryptOffIntStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	N/A	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	AVG	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	N/A	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	N/A	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	N/A	
SOURCE_IP_ADDRESSES	INTEGER	No	The source IP port of the table entry.	True	AVG	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	N/A	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	AVG	
DEST_IP_PORT	INTEGER	No	The destination IP address of the table entry.	True	AVG	

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	CLI Command Reference
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	AVG	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A	

SBX5KLicenseUsageStats

Name	Type	Index	Description	canAggregate
FEATURE_NAME	STRING	Yes	The name of the feature.	False
LICENSE_MODE	STRING	False	Displays the licensing mode of SBC Core.	False
ENCRYPT_ENABLED	INTEGER	False	Set based on whether encrypt license is available at the SBC Core.	False
SRTP_ENABLED	INTEGER	False	Set based on whether srtp license is available at the SBC Core.	False
VIDEO_ENABLED	INTEGER	False	Set based on whether video license is available at the SBC Core.	False
AMRNB_ENABLED	INTEGER	False	Set based on whether amrnb license is available at the SBC Core.	False
AMRWB_ENABLED	INTEGER	False	Set based on whether amrwb license is available at the SBC Core.	False
EVRC_ENABLED	INTEGER	False	Set based on whether evrc license is available at the SBC Core.	False
NICE_ENABLED	INTEGER	False	Set based on whether nicerec license is available at the SBC Core.	False

Name	Type	Index	Description	canAggregate
MRF_ENABLED	INTEGER	False	Set based on whether mrf license is available at the SBC Core.	False
SIPREC_ENABLED	INTEGER	False	Set based on whether siprec license is available at the SBC Core.	False
VDSPRTU_ENABLED	INTEGER	False	Set based on whether transcode license is available at the SBC Core.	False
PDCS_ENABLED	INTEGER	False	Set based on whether pdcs license is available at the SBC Core.	False
LI_ENABLED	INTEGER	False	Set based on whether LI license is available at the SBC Core.	False
RTU_ENABLED	INTEGER	False	Set based on whether SBC Core-RTU license is available at the SBC Core.	False
DSPG722_ENABLED	INTEGER	False	Set based on whether DSPG722license is available at the SBC Core.	False
GMP4X1_ENABLED	INTEGER	False	Set based on whether GMP4X1 license is available at the SBC Core.	False
SIPI_ENABLED	INTEGER	False	Set based on whether SIPI license is available at the SBC Core.	False
SIP323_ENABLED	INTEGER	False	Set based on whether SIP323 license is available at the SBC Core.	False
GMP1X10_ENABLED	INTEGER	False	Set based on whether 1X10GMP license is available at the SBC Core.	False
POLRTU_ENABLED	INTEGER	False	Set based on whether POLRTU license is available at the SBC Core.	False

Name	Type	Index	Description	canAggregate
PSXRTU_ENABLED	INTEGER	False	Set based on whether PSXRTU license is available at the SBC Core.	False
CAPACITY_ENABLED	INTEGER	False	Set based on whether CAPACITY license is available at the SBC Core.	False
E911_ENABLED	INTEGER	False	Set based on whether E911 license is available at the SBC Core.	False
ENUM_ENABLED	INTEGER	False	Set based on whether ENUM license is available at the SBC Core.	False
SWINSTANCE_ENABLED	INTEGER	False	Set based on whether SWINSTANCE license is available at the SBC Core.	False
EVS_ENABLED	INTEGER	False	Set based on whether EVS license is available at the SBC Core.	False
SILK_ENABLED	INTEGER	False	Set based on whether SILK license is available at the SBC Core.	False
LBINSTANCE_ENABLED	INTEGER	False	Set based on whether SLB license is available at the SLB.	False
SLBSESS_ENABLED	INTEGER	False	Set based on whether SLB sessions license is available at the SBC.	False
MEDIA_PROBE_AUTH	INTEGER	False	Set based on whether MEDIA PROBE license is available at the SBC.	False
WEB_SOCKET_AUTH	INTEGER	False	Set based on whether WEB SOCKET license is available at the SBC.	False
NOTRUF_AUTH	INTEGER	False	Set based on whether NOTRUF license is available at the SBC.	False

Name	Type	Index	Description	canAggregate
CE_NAME	STRING	False	The name of the compute element for this entry.	False
T140	INTEGER	False	Set based on whether the t140 code is used on at least one call leg for the current interval.	False
DOD	INTEGER	False	Set based on when the application is running in DOD mode.	False
FIPS	INTEGER	False	Set based on when the application is running in FIPS mode.	False
CNEINSTANCE_ENABLED	INTEGER	False	Set based on whether cneInstance license is available at the SBC.	True

SBX5KMediaOffIntStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	N/A	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	AVG	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	N/A	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	N/A	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	N/A	
SOURCE_IP_ADDRESSES	INTEGER	No	The source IP port of the table entry.	True	AVG	

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	CLI Command Reference
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	N/A	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	AVG	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	N/A	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	AVG	
ETHER_TYPE	COUNTER	No	The first ether type found in the Ethernet packet.	True	SUM	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	SUM	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A	

SBX5KMtrmConnPortPeerStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Zone - MTRM Conn Port - CLI
ZNAME	STRING	Yes	The name of the address context zone.	
STAT_INDEX	GAUGE	Yes	Master Trunk Group Connection Port index.	

Column Name	Column Type	Index	Description	CLI Command Reference
PEER_INDEX	INTEGER	Yes	Peer connection index.	
RTO	INTEGER	No	The current Retransmission Time Out in seconds. The messages that are in the retransmission buffer send at this interval.	
IRRT_BUFFER_DEPTH	INTEGER	No	The infinite retry retransmission buffer. The messages in this buffer attempt to send to the peer as long as the connection is alive. If the connection to the peer is lost this buffer is flushed.	
FRRT_BUFFER_DEPTH	INTEGER	No	The finite retry retransmission buffer. The messages in this buffer attempt to send to the server twice. Failure to send this message to the server results in the message being discarded. If the connection to the peer is lost this buffer is flushed.	
MSGs_SENT	INTEGER	No	The total number of messages sent on this port.	
MSGs_RCVD	INTEGER	No	The total number of messages received on this port.	
SHELF_REG_REQ_MSGS_SENT	INTEGER	No	The number of Shelf Registration Request messages sent on this port.	
SHELF_REG_REQ_MSGS_RCVD	INTEGER	No	The number of Shelf Registration Request messages received on this port.	

Column Name	Column Type	Index	Description	CLI Command Reference
SHELF_REG_RESP_MSGS_SENT	COUNTER	No	The number of Shelf Registration Response messages sent on this port.	
SHELF_REG_RESP_MSGS_RCVD	COUNTER	No	The number of Shelf Registration Response messages received on this port.	
HEALTH_CHECK_REQ_MSGS_SENT	COUNTER	No	The number of Health Check messages sent from this port.	
HEALTH_CHECK_REQ_MSGS_RCVD	COUNTER	No	The number of Health Check Request messages received on this port.	
HEALTH_CHECK_RESP_MSGS_SENT	COUNTER	No	The number of Health Check Response messages sent on this port.	
HEALTH_CHECK_RESP_MSGS_RCVD	COUNTER	No	The number of Health Check Response messages received on this port.	
MTRG_REG_REQ_MSGS_SENT	COUNTER	No	The number of MTRG Reg Request messages sent from this port.	
MTRG_REG_REQ_MSGS_RCVD	COUNTER	No	The number of MTRG Reg Request messages received on this port.	
MTRG_REG_RESP_MSGS_SENT	COUNTER	No	The number of MTRG Reg Response messages sent on this port.	
MTRG_REG_RESP_MSGS_RCVD	COUNTER	No	The number of MTRG Reg Response messages received on this port.	

Column Name	Column Type	Index	Description	CLI Command Reference
IP_AUDIT_REQ_MSGS_SENT	COUNTER	No	The number of IP Audit Reg Request messages sent from this port.	
IP_AUDIT_REQ_MSGS_RCVD	COUNTER	No	The number of IP Audit Request messages received on this port.	
IP_AUDIT_RESP_MSGS_SENT	COUNTER	No	The number of IP Audit Response messages sent on this port.	
IP_AUDIT_RESP_MSGS_RCVD	COUNTER	No	The number of IP Audit Response messages received on this port.	
BW_ALLOC_REQ_MSGS_SENT	COUNTER	No	The number of Bandwidth Alloc Request messages sent from this port.	
BW_ALLOC_REQ_MSGS_RCVD	COUNTER	No	The number of Bandwidth Alloc Request messages received on this port.	
BW_ALLOC_RESP_MSGS_SENT	COUNTER	No	The number of Bandwidth Alloc Response messages sent on this port.	
BW_ALLOC_RESP_MSGS_RCVD	COUNTER	No	The number of Bandwidth Alloc Response messages received on this port.	
CALL_ALLOC_REQ_MSGS_SENT	COUNTER	No	The number of Call Alloc Request messages sent from this port.	
CALL_ALLOC_REQ_MSGS_RCVD	COUNTER	No	The number of Call Alloc Request messages received on this port.	
CALL_ALLOC_RESP_MSGS_SENT	COUNTER	No	The number of Call Alloc Response messages sent on this port.	

Column Name	Column Type	Index	Description	CLI Command Reference
CALL_ALLOC_RESP_MSGS_RCVD	COUNTER	No	The number of Call Alloc Response messages received on this port.	
BW_FREE_REQ_MSGS_SENT	COUNTER	No	The number of Bandwidth Free Request messages sent from this port.	
BW_FREE_REQ_MSGS_RCVD	COUNTER	No	The number of Bandwidth Free Request messages received on this port.	
CALL_FREE_REQ_MSGS_SENT	COUNTER	No	The number of Call Free Request messages sent from this port.	
CALL_FREE_REQ_MSGS_RCVD	COUNTER	No	The number of Call Free Request messages received on this port.	
TAKE_BACK_BW_IND_MSGS_SENT	COUNTER	No	The number of Takeback Bandwidth Indication messages sent from this port.	
TAKE_BACK_BW_IND_MSGS_RCVD	COUNTER	No	The number of Takeback Bandwidth Indication messages received on this port.	
TAKE_BACK_CALLS_IND_MESSAGES_SENT	COUNTER	No	The number of Takeback Call Indication messages sent from this port.	
TAKE_BACK_CALLS_IND_MESSAGES_RCVD	COUNTER	No	The number of Takeback Call Indication messages received on this port.	
MTRG_DEREG_REQ_MSGS_SENT	COUNTER	No	The number of MTRG Dereg Request messages sent from this port.	
MTRG_DEREG_REQ_MSGS_RCVD	COUNTER	No	The number of MTRG Dereg Request messages received on this port.	

Column Name	Column Type	Index	Description	CLI Command Reference
MTRG_UNAVAILABLE_MSGS_SENT	COUNTER	No	The number of MTRG Unavailable messages sent from this port.	
MTRG_UNAVAILABLE_MSGS_RECEIVED	COUNTER	No	The number of MTRG Unavailable messages received on this port.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

SBX5KRogueMediaIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
ETHER_TYPE	INTEGER	No	The first ether type found in the Ethernet packet.	True	
DISCARD_COUNTER	COUNTER	No	The number of packets discarded by the policer.	True	
RING_TYPE	INTEGER	No	The media ring type.	False	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

SBX5KSipByeResponseIntervalStats

Name	Type	Index	Description	canAggregate
ACNAME	STRING	True	The name of the address context.	False
ZNAME	STRING	True	The name of the address context zone.	False
NAME	STRING	True	The name of this SIP peer group.	False
BYE_RESPONSE_401	COUNTER	False	Indicates the total number of (interval) 401 responses for received Bye messages.	True
BYE_RESPONSE_403	COUNTER	False	Indicates the total number of (interval) 403 responses for received Bye messages.	True
BYE_RESPONSE_407	COUNTER	False	Indicates the total number of (interval) 407 responses for received Bye messages.	True

Name	Type	Index	Description	canAggregate
BYE_RESPONSE_481	COUNTER	False	Indicates the total number of (interval) 481 responses for received Bye messages.	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SBX5KSipInviteResponseIntervalStats

Name	Index	Type	Description	CanAggregate
ACNAME	True	STRING	The name of the address context.	False
ZNAME	True	STRING	The name of the address context zone.	False
NAME	True	STRING	The name of this SIP peer group.	False
INV_RESPONSE_401	False	COUNTER	Indicates the total number of (interval) 401 responses for received Invite messages.	True
INV_RESPONSE_403	False	COUNTER	Indicates the total number of (interval) 403 responses for received Invite messages.	True
INV_RESPONSE_407	False	COUNTER	Indicates the total number of (interval) 407 responses for received Invite messages.	True
INV_RESPONSE_481	False	COUNTER	Indicates the total number of (interval) 481 responses for received Invite messages.	True
CE_NAME	False	STRING	The name of the compute element for this entry.	False

SBX5KSipIpPeerIntervalStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	IP Policing - CLI

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ZNAME	STRING	Yes	The name of the address context zone.	False	
NAME	STRING	Yes	The name of this SIP peer group.	False	
INBOUND_SESSIONS	COUNTER	False	Indicates the total number of (interval) calls routed to this peer.	True	
INBOUND_CPS	COUNTER	False	Indicates the total number of (interval) calls routed to this peer per second.	True	
TOTAL_INBOUND_SESSIONS	COUNTER	False	Indicates the total number of (interval) inbound active sessions.	True	
OUTBOUND_SESSIONS	COUNTER	False	Indicates the total number of (interval) calls initiated by this peer.	True	
OUTBOUND_CPS	COUNTER	False	Indicates the total number of (interval) calls initiated by this peer per second.	True	
CE_NAME	STRING	False	The name of the compute element for this entry.	False	

SBX5KSipOptResponseIntervalStats

Name	Index	Type	Description	canAggregate
ACNAME	True	STRING	The name of the address context.	False
ZNAME	True	STRING	The name of the address context zone.	False

Name	Index	Type	Description	canAggregate
NAME	True	STRING	The name of this SIP peer group.	False
OPT_RESPONSE_401	False	COUNTER	Indicates the total number of (interval) 401 responses for received Option messages.	True
OPT_RESPONSE_403	False	COUNTER	Indicates the total number of (interval) 403 responses for received Option messages.	True
OPT_RESPONSE_407	False	COUNTER	Indicates the total number of (interval) 407 responses for received Option messages.	True
OPT_RESPONSE_481	False	COUNTER	Indicates the total number of (interval) 481 responses for received Option messages.	True
CE_NAME	False	STRING	The name of the compute element for this entry.	False

SBX5KSipRegResponseIntervalStats

Name	Index	Type	Description	canAggregate
ACNAME	True	STRING	The name of the address context.	False
ZNAME	True	STRING	The name of the address context zone.	False
NAME	True	STRING	The name of this SIP peer group.	False
REG_RESPONSE_401	False	COUNTER	Indicates the total number of (interval) 401 responses for received Register messages.	True
REG_RESPONSE_403	False	COUNTER	Indicates the total number of (interval) 403 responses for received Register messages.	True
REG_RESPONSE_407	False	COUNTER	Indicates the total number of (interval) 407 responses for received Register messages.	True

Name	Index	Type	Description	canAggregate
REG_RESPONSE_481	False	COUNTER	Indicates the total number of (interval) 481 responses for received Register messages.	True
CE_NAME	False	STRING	The name of the compute element for this entry.	False

SBX5KSrtpDecryptOffIntStat

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	No	The source IP address of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	INTEGER	No	The destination IP port of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
ETHER_TYPE	INTEGER	No	The first ether type found in the Ethernet packet.	True	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

SBX5KSystemDspStatusDspUsageStats

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
SYSTEM_NAME	STRING	True	Name of the system.		Show Status System
COMPRESSION_TOTAL	INTEGER	False	Total compression resource capacity on this server.		
COMPRESSION_UTILIZATION	INTEGER	False	Percentage utilization of compression resources on this server.		
COMPRESSION_ALLOC_FAILURES	INTEGER	False	Percentage of compression resources allocation failures on this server.		
G711_TOTAL	INTEGER	False	Total G711 resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711_UTILIZATION	INTEGER	False	Percentage utilization of G711 resources on this server.		
G726_TOTAL	INTEGER	False	Total G726 resource capacity on this server.		
G726_UTILIZATION	INTEGER	False	Percentage utilization of G726 resources on this server.		
G729AB_TOTAL	INTEGER	False	Total G729A+B resource capacity on this server.		
G729AB_UTILIZATION	INTEGER	False	Percentage utilization of G729A+B resources on this server.		
G7231_TOTAL	INTEGER	False	Total G723.1 resource capacity on this server.		
G7231_UTILIZATION	INTEGER	False	Percentage utilization of G7231 resources on this server.		
ILBC_TOTAL	INTEGER	False	Total iLBC resource capacity on this server.		
ILBC_UTILIZATION	INTEGER	False	Percentage utilization of iLBC resources on this server.		
ILBC_ALLOC_FAILURES	INTEGER	False	Percentage of iLBC resources allocation failures on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
ECM_TOTAL	INTEGER	False	Total T.38 ECM resource capacity on this server.		
ECM_UTILIZATION	INTEGER	False	Percentage utilization of T.38 ECM resources on this server.		
ECM_ALLOC_FAILURES	INTEGER	False	Percentage of T.38 ECM resources allocation failures on this server.		
TONE_TOTAL	INTEGER	False	Total tone resource capacity on this server.		
TONE_UTILIZATION	INTEGER	False	Percentage utilization of tone resources on this server.		
TONE_ALLOC_FAILURES	INTEGER	False	Percentage of tone resource allocation failures on this server.		
EVRCB0_TOTAL	INTEGER	False	Total EVRCB0 resource capacity on this server.		
EVRCB0_UTILIZATION	INTEGER	False	Percentage utilization of EVRCB0 resources on this server.		
EVRCB0_ALLOC_FAILURES	INTEGER	False	Percentage of EVRCB0 resources allocation failures on this server.		
AMRNB_TOTAL	INTEGER	False	Total AMR-NB resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
AMRNB_UTILIZATION	INTEGER	False	Percentage utilization of AMR-NB resources on this server.		
AMRNB_ALLOC_FAILURES	INTEGER	False	Percentage of AMR-NB resources allocation failures on this server.		
AMRWB_TOTAL	INTEGER	False	Total AMR-WB resource capacity on this server.		
AMRWB_UTILIZATION	INTEGER	False	Percentage utilization of AMR-WB resources on this server.		
AMRWB_ALLOC_FAILURES	INTEGER	False	Percentage of AMR-WB resources allocation failures on this server.		
G722_TOTAL	INTEGER	False	Total G.722 resource capacity on this server.		
G722_UTILIZATION	INTEGER	False	Percentage utilization of G.722 resources on this server.		
G722_ALLOC_FAILURES	INTEGER	False	Percentage of G.722 resources allocation failures on this server.		
EVRC0_TOTAL	INTEGER	False	Total EVRC0 resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
EVRC0_UTILIZATION	INTEGER	False	Percentage utilization of EVRC0 resources on this server.		
EVRC0_ALLOC_FAILURES	INTEGER	False	Percentage of EVRC0 resources allocation failures on this server.		
COMPRESSION_AVAILABLE	INTEGER	False	Number of compression resources currently unused and available on this server.		
TONE_AVAILABLE	INTEGER	False	Number of tone resources currently unused and available on this server.		
G7221_TOTAL	INTEGER	False	Total G.722.1 resource capacity on this server.		
G7221_UTILIZATION	INTEGER	False	Percentage utilization of G.722.1 resources on this server.		
EFR_TOTAL	INTEGER	False	Total EFR resource capacity on this server.		
EFR_UTILIZATION	INTEGER	False	Percentage utilization of EFR resources on this server.		
G711SS_TOTAL	INTEGER	False	Total G711SS (silence suppression) resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SS_UTILIZATION	INTEGER	False	Percentage utilization of G711SS (silence suppression) resources on this server.		
SLOT1_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
SLOT2_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
SLOT3_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
SLOT4_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
G711V8_TOTAL	INTEGER	False	Total G711 V8 resource capacity on this server.		
G711V8_UTILIZATION	INTEGER	False	Percentage utilization of G711 V8 resources on this server.		
G711SSV8_TOTAL	INTEGER	False	Total G711SS (silence suppression) V8 resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SSV8_UTILIZATION	INTEGER	False	Percentage utilization of G711SS (silence suppression) V8 resources on this server.		
G726V8_TOTAL	INTEGER	False	Total G726 V8 resource capacity on this server.		
G726V8_UTILIZATION	INTEGER	False	Percentage utilization of G726 V8 resources on this server.		
G7231V8_TOTAL	INTEGER	False	Total G723.1 V8 resource capacity on this server.		
G7231V8_UTILIZATION	INTEGER	False	Percentage utilization of G7231 V8 resources on this server.		
G722V8_TOTAL	INTEGER	False	Total G.722 V8 resource capacity on this server.		
G722V8_UTILIZATION	INTEGER	False	Percentage utilization of G.722 V8 resources on this server.		
G7221V8_TOTAL	INTEGER	False	Total G.722.1 V8 resource capacity on this server.		
G7221V8_UTILIZATION	INTEGER	False	Percentage utilization of G.722.1 V8 resources on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G729ABV8_TOTAL	INTEGER	False	Total G729A+B V8 resource capacity on this server.		
G729ABV8_UTILIZATION	INTEGER	False	Percentage utilization of G729A+B V8 resources on this server.		
ECMV34_TOTAL	INTEGER	False	Total T.38 ECM V.34 resource capacity on this server.		
ECMV34_UTILIZATION	INTEGER	False	Percentage utilization of T.38 ECM V.34 resources on this server.		
ILBCV8_TOTAL	INTEGER	False	Total iLBC V8 resource capacity on this server.		
ILBCV8_UTILIZATION	INTEGER	False	Percentage utilization of iLBC V8 resources on this server.		
OPUS_TOTAL	INTEGER	False	Total OPUS resource capacity on this server.		
OPUS_UTILIZATION	INTEGER	False	Percentage utilization of OPUS resources on this server.		
OPUS_ALLOC_FAILURES	INTEGER	False	Percentage of OPUS resources allocation failures on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
USAGE_EVS_TOTAL	INTEGER	False	The total EVS resource capacity on this server.		
USAGE_EVS_UTILIZATION	INTEGER	False	The percentage utilization of EVS resources on this server.		
USAGE_SILK8_TOTAL	COUNT	False	Total SILK_8 resource capacity on the present server		
USAGE_SILK8_UTILIZATION	COUNT	False	Percentage utilization of SILK_8 resources on the present server		
USAGE_SILK16_TOTAL	COUNT	False	Total SILK_16 resource capacity on the present server		
USAGE_SILK16_UTILIZATION	COUNT	False	Percentage utilization of SILK_16 resources on the present server		
USAGE_AMR_NBT140_TOTAL	INTEGER	True	Total AMR-NB with T.140 resource capacity in the server.		
USAGE_AMR_NBT140_UTILIZATION	INTEGER	False	The utilization percentage of AMR-NB with T.140 resource in the server.		
USAGE_AMR_WBT140_TOTAL	INTEGER	False	Total AMR-WB with T.140 resource capacity in the server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
USAGE_AMR_WBT140_UTILIZATION	INTEGER	False	The utilization percentage of AMR-WB with T.140 resource in the server.		
COMP_HP_UTILIZATION	INTEGER	False	Percentage utilization of AMR-WB with T.140 resource on this server.		
RESOURCE_HP_UTILIZATION	INTEGER	False	Percentage utilization of tone resources used for high priority calls on this server.		
DSP_EVS_T140_TOTAL	INTEGER	False	Total EVS with T.140 resource capacity on this server.		
DSP_EVS_T140_UTILIZATION	INTEGER	False	Percentage utilization of EVS with T.140 resources on this server		
G711T140_TOTAL	GAUGE	False	The total G711 with T.140 resource capacity on this server.	MEAN	
G711T140_UTILIZATION	GAUGE	False	The percentage utilization of G711 with T.140 resources on this server.	MEAN	
G711SST140_TOTAL	GAUGE	False	The total G711SS with T.140 resource capacity on this server.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SST140_UTILIZATION	GAUGE	False	The percentage utilization of G711SS with T.140 resources on this server.	MEAN	
OPUST140_TOTAL	GAUGE	False	The total Opus with T.140 resource capacity on this server.	MEAN	
OPUST140_UTILIZATION	GAUGE	False	The percentage utilization of Opus with T.140 resources on this server.	MEAN	
G722T140_TOTAL	GAUGE	False	The total G722 with T.140 resource capacity on this server.	MEAN	
G722T140_UTILIZATION	GAUGE	False	The percentage utilization of G722 with T.140 resources on this server.	MEAN	
G722V8T140_TOTAL	GAUGE	False	The total G722 V8 with T.140 resource capacity on this server.	MEAN	
G722V8T140_UTILIZATION	GAUGE	False	The percentage utilization of G722 V8 with T.140 resources on this server.	MEAN	
G711V8T140_TOTAL	GAUGE	False	The total G711 V8 with T.140 resource capacity on this server.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711V8T140_UTILIZATION	GAUGE	False	The percentage utilization of G711 V8 with T.140 resources on this server.	MEAN	
G711SSV8T140_TOTAL	GAUGE	False	The total G711SS V8 with T.140 resource capacity on this server.	MEAN	
G711SSV8T140_UTILIZATION	GAUGE	False	The percentage utilization of G711SS V8 with T.140 resources on this server.	MEAN	
L16_TOTAL	GAUGE	False	The total L16 resource capacity on this server.	MEAN	
L16_UTILIZATION	GAUGE	False	The percentage utilization of L16 resources on this server.	MEAN	
CE_NAME	STRING	False	The name of the compute element for this entry.	N/A	

SBX5KUflowOffListIntStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	N/A	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	AVG	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	N/A	

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	CLI Command Reference
INTERFAC E_GROUP_ NAME	STRING	No	The name of the interface group of the table entry.	True	N/A	
INTERFAC E_NAME	STRING	No	The name of the interface of the table entry.	True	N/A	
SOURCE_I P_ADDRES S	STRING	No	The source IP port of the table entry.	True	N/A	
DEST_IP_A DDRESS	STRING	No	The destination IP address of the table entry.	True	N/A	
SOURCE_I P_PORT	INTEGER	No	The source IP port of the table entry.	True	AVG	
DEST_IP_P ORT	STRING	No	The destination IP address of the table entry.	True	N/A	
IP_PROTO COL	INTEGER	No	The IP Protocol of the table entry.	True	AVG	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A	

Shared CAC Stats

SharedCacFailureIntStats

Column Name	Column Type	Index	Description	canAggregate
NAME	STRING	True	The name of this shared CAC-limits pool.	False

Column Name	Column Type	Index	Description	canAggregate
ALLOC_FAIL_BW_LIMIT	GAUGE	False	The number of BW Requests which fail because the specified interval for this shared CAC limits pool exceeds the configured bandwidth limit.	True
ALLOC_FAIL_CALL_LIMIT	GAUGE	False	The number of BW Requests which fail because the specified interval for this shared CAC limits pool exceeds the configured call limit.	False
ALLOC_FAIL_PARENT_CONSTRAINT	GAUGE	False	The current number of failures because of a parent limit denial for the specified interval.	False
ALLOC_FAIL_SIP_REG	GAUGE	False	The number of SIP registration attempts that fail because the specified interval for this shared CAC limits pool exceeds the configured registration limit.	False
SIP_SUBS_FAIL_POLICING	GAUGE	False	The current number of SIP Subscribe attempts that failed due to policing on a trunk group.	False
SIP_OTHER_REQ_FAIL_POLICING	GAUGE	False	The current number of SIP other non-invite attempts that failed due to policing on a trunk group.	False
VIDEO_THRESHOLD_LIMIT	COUNTER	False	The number of exceeded video threshold limits for this shared CAC limits pool.	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SharedCacIntervalStatistics

Column Name	Column Type	Index	Description	canAggregate
NAME	STRING	True	The name of this shared CAC-limits pool.	False

Column Name	Column Type	Index	Description	canAggregate
MAX_ACTIVE_CALLS	GAUGE	False	The current high watermark of total number of active calls in both the inbound and outbound directions using limits from this shared CAC limits pool.	False
IN_BW_USAGE	GAUGE	False	The sum of BW usage (expected data rate in bits per second multiplied by call duration in seconds) for every inbound call associated with this shared CAC limits pool for the specified interval.	False
OUT_BW_USAGE	GAUGE	False	The sum of BW usage (expected data rate in bits per second multiplied by call duration in seconds) for every outbound call associated with this shared CAC limits pool for the specified interval.	False
MAX_ACTIVE_BW_USAGE	GAUGE	False	The high watermark of BW usage in either direction associated with this shared CAC limits pool for the specified interval.	False
ACTIVE_REGS	GAUGE	False	The current number of active registrations of this shared CAC-limits pool.	False
MAX_ACTIVE_REGS	GAUGE	False	The number of maximum active registrations of this shared CAC-limits pool (this is the high-watermark achieved on this pool during this interval).	False
ACTIVE_SUBS	GAUGE	False	The current number of active subscriptions on this shared CAC-limits pool.	False
MAX_ACTIVE_SUBS	GAUGE	False	The current number of maximum active subscriptions on this shared CAC-limits pool. (This is the high-watermark achieved on this shared CAC).	False
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SIP Stats

SipIntervalStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ZNAME	STRING	Yes	The name of the address context zone.	False	
NAME	STRING	Yes	The name of this SIP trunk group.	True	
RCV_INVITE	COUNTER	No	Indicates the total number of (interval) received Invite messages.	False	
SND_INVITE	COUNTER	No	Indicates the total number of (interval) sent Invite messages.	True	
RCV_ACK	COUNTER	No	Indicates the total number of (interval) Received Ack.	True	
SND_ACK	COUNTER	No	Indicates the total number of (interval) Sent Ack messages.	True	
RCV_PRACK	COUNTER	No	Indicates the total number of (interval) received Prack messages.	True	
SND_PRACK	COUNTER	No	Indicates the total number of (interval) sent Prack messages.	True	
RCV_INFO	COUNTER	No	Indicates the total number of (interval) received INFO messages.	True	
SND_INFO	COUNTER	No	Indicates the total number of (interval) sent INFO messages.	True	
RCV_REFERER	COUNTER	No	Indicates the total number of (interval) received Refer messages.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SND_REFER	COUNTER	No	Indicates the total number of (interval) sent Refer messages.	True	
RCV_BYE	COUNTER	No	Indicates the total number of (interval) Received Bye messages.	True	
SND_BYE	COUNTER	No	Indicates the total number of (interval) sent Bye messages.	True	
RCV_CANCEL	COUNTER	No	Indicates the total number of (interval) received Cancel messages.	True	
SND_CANCEL	COUNTER	No	Indicates the total number of (interval) sent Cancel messages.	True	
RCV_REGISTER	COUNTER	No	Indicates the total number of (interval) received Register messages.	True	
SND_REGISTER	COUNTER	No	Indicates the total number of (interval) sent Register messages.	True	
RCV_UPDATE	COUNTER	No	Indicates the total number of (interval) received Update messages.	True	
SND_UPDATE	COUNTER	No	Indicates the total number of (interval) sent Update messages.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
RCV18_X	COUNTER	No	Indicates the total number of (interval) received 18x messages.	True	
SND18_X	COUNTER	No	Indicates the total number of (interval) sent 18x messages.	True	
RCV1_XX	COUNTER	No	Indicates the total number of (interval) received 1xx messages except 18x messages.	True	
SND1_XX	COUNTER	No	Indicates the total number of (interval) sent 1xx messages except 18x messages.	True	
RCV2_XX	COUNTER	No	Indicates the total number of (interval) received 2xx (Invite) messages.	True	
SND2_XX	COUNTER	No	Indicates the total number of (interval) sent 2xx (Invite) messages.	True	
RCV_NON_I NV2_XX	COUNTER	No	Indicates the total number of (interval) received 2xx (Non-Invite) messages.	True	
SND_NON_I NV2_XX	COUNTER	No	Indicates the total number of (interval) sent 2xx (Non-Invite) messages.	True	
RCV3_XX	COUNTER	No	Indicates the total number of (interval) received 3xx messages.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SND3_XX	COUNTER	No	Indicates the total number of (interval) sent 3xx messages.	True	
RCV4_XX	COUNTER	No	Indicates the total number of (interval) received 4xx messages.	True	
SND4_XX	COUNTER	No	Indicates the total number of (interval) sent 4xx messages.	True	
RCV5_XX	COUNTER	No	Indicates the total number of (interval) receive 5xx messages.	True	
SND5_XX	COUNTER	No	Indicates the total number of (interval) sent 5xx messages.	True	
RCV6_XX	COUNTER	No	Indicates the total number of (interval) receive 6xx messages.	True	
SND6_XX	COUNTER	No	Indicates the total number of (interval) sent 6xx messages.	True	
RCV_NON_INV_ERR	COUNTER	No	Indicates the total number of (interval) receive Nonlvite Error messages.	True	
SND_NON_INV_ERR	COUNTER	No	Indicates the total number of (interval) sent Nonlvite Error messages.	True	
RCV_UNKNOWN_MSG	COUNTER	No	Indicates the total number of (interval) receive Unknown messages.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
RCV_SUBSC RIBER	COUNTER	No	Indicates the total number of (interval) receive Subscriber messages.	True	
SND_SUBSC RIBER	COUNTER	No	Indicates the total number of (interval) sent Subscriber messages.	True	
RCV_NOTIF Y	COUNTER	No	Indicates the total number of (interval) receive Notify messages.	True	
SND_NOTIF Y	COUNTER	No	Indicates the total number of (interval) sent Notify messages.	True	
RCV_OPTIO N	COUNTER	No	Indicates the total number of (interval) receive Option messages.	True	
SND_OPTIO N	COUNTER	No	Indicates the total number of (interval) sent Option messages.	True	
INV_RE_TRA NSMIT	COUNTER	No	Indicates the total number of (interval) Invite messages Re-Transmitted.	True	
REG_RE_TR ANSMIT	COUNTER	No	Indicates the total number of (interval) Register messages Re-Transmitted.	True	
BYE_RETRA NSMIT	COUNTER	No	Indicates the total number of (interval) Bye messages Re-Transmitted.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
CANCLE_RE_TRANSMIT	COUNTER	No	Indicates the total number of (interval) Cancel messages Re-Transmitted.	True	
OTHER_RE_TRANSMIT	COUNTER	No	Indicates the total number of (interval) Other messages Re-Transmitted.	True	
RCV_MESSAGE	COUNTER	No	Indicates the total number of (interval) received Message method.	True	
SEND_MESSAGE	COUNTER	No	Indicates the total number of (interval) sent Message method.	True	
RCV_PUBLISH	COUNTER	No	Indicates the total number of (interval) received Publish method.	True	
SEND_PUBLISH	COUNTER	No	Indicates the total number of (interval) sent Publish method.	True	
EMERGENCY_ACCEPT	COUNTER	No	Indicates the total number of (interval) emergency calls accepted.	True	
EMERGENCY_REJECT_BWCALL	COUNTER	No	Indicates the total number of (interval) emergency calls rejected because of bandwidth limit or call limit.	True	
EMERGENCY_REJECT_POLICER	COUNTER	No	Indicates the total number of (interval) emergency calls rejected because of Priority Policer.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
HPC_ACCEPT	COUNTER	No	Indicates the total number of (interval) HPC calls accepted.	True	
NUM_OF_CALLS_SENDING_AARS	COUNTER	No	Indicates the number of calls sending AAR requests.	True	
NUM_OF_RECEIVED_AAA_FAILURES	COUNTER	No	Indicates the number of received AAA failures.	True	
NUM_OF_RECEIVED_AAA_SUCCESSES	COUNTER	No	Indicates the number of received AAA Successes.	True	
NUM_OF_TOTAL_AAR_SENT	COUNTER	No	Indicates the total number of AAR messages sent.	True	
NUM_OF_TIMEOUT_OR_ERROR_AAR	COUNTER	No	Indicates the number of AAR messages not answered.	True	
NUM_OF_RECEIVED_RARS	COUNTER	No	Indicates the number of RAR messages received.	True	
NUM_OF_RECEIVED_ASRS	COUNTER	No	Indicates the number of ASR messages received.	True	
NUM_OF_SENT_STRS	COUNTER	No	Indicates the number of STR messages sent.	True	
EMERGENCY_REG_ACCEPT	COUNTER	No	Indicates the number of (interval) emergency registrations accepted.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
EMERGENCY_REG_REJECT_LIMIT	COUNTER	No	Indicates the number of (interval) emergency registrations rejected because of the registration limit.	True	
EMERGENCY_REG_REJECT_POLICER	COUNTER	No	Indicates the number of (interval) emergency registrations rejected because of the Priority Policer.	True	
EMERGENCY_OOD_ACCEPT	COUNTER	No	Indicates the number of (interval) emergency OOD Requests accepted.	True	
EMERGENCY_OOD_REJECT_POLICER	COUNTER	No	Indicates the number of (interval) emergency OOD Requests rejected because of the Priority Policer.	True	
EMERGENCY_SUBSCRIBE_ACCEPT	COUNTER	No	Indicates the number of (interval) emergency Subscribe Requests accepted.	True	
EMERGENCY_SUBS_REJECT_LIMIT	COUNTER	No	Indicates the number of (interval) emergency Subscribe Requests rejected because of the subscription limit.	True	
EMERGENCY_SUBS_REJECT_POLICER	COUNTER	No	Indicates the number of (interval) emergency Subscribe Requests rejected because of the Priority Policer.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
PARSE_ERROR	COUNTER	No	Indicates the total number of (interval) Parse Errors.	True	
NUM_OF_TOTAL_UDR_SENT	COUNTER	No	Indicates the total number of UDR messages sent.	True	
NUM_OF_TIMEOUT_UDR_ERROR	COUNTER	No	Indicates the number of UDR messages not answered.	True	
NUM_OF_RECEIVED_UDASUCCESS	COUNTER	No	Indicates the number of received UDA success	True	
NUM_OF_RECEIVED_UDAFAILURE	COUNTER	No	Indicates the number of received UDA failures.	True	
TOTAL_NUM_S8HR_OUT_REG	COUNTER	No	Indicates the total number (includes success and failed) of registration received from S8HR Outbound Roaming Users.	True	
NUM_S8HR_OUT_REG_SUCCESS	COUNTER	No	Indicates the number of successful registration from S8HR Outbound Roaming Users.	True	
NUM_S8HR_OUT_REG_FAILURE	COUNTER	No	Indicates the number of S8HR Outbound Roaming Users registrations failed.	True	
TOTAL_NUM_S8HR_OT_NML_CALL	COUNTER	No	Indicates the total number of normal calls initiated from S8HR Outbound Roaming Users.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
NUM_OF_S8 HR_OT_NML _CALL_SUC	COUNTER	No	Indicates the number of successful normal calls from S8HR Outbound Roaming Users.	True	
NUM_OF_S8 HR_OT_NML _CALL_FAIL	COUNTER	No	Indicates the total number of failed normal calls from S8HR Outbound Roaming Users.	True	
NUM_OF_S8 HR_OT_EMG _CALL_REJ	COUNTER	No	Indicates the number of S8HR Outbound Roaming User's emergency calls rejected.	True	
NUM_OF_S8 HR_IN_EMG _REG_SUC	COUNTER	No	Indicates the number of Successful registration from S8HR Inbound Roaming Users.	True	
NUM_OF_S8 HR_IN_EMG _REG_FAIL	COUNTER	No	Indicates the number of S8HR Inbound User's registration rejected.	True	
NUM_OF_S8 HR_IN_EMG _CALL_SUC	COUNTER	No	Indicates the number of successful emergency calls from S8HR Inbound User.	True	
NUM_OF_S8 HR_IN_EMG _CALL_FAIL	COUNTER	No	Indicates the number of S8HR Inbound Users emergency calls failed.	True	
NUM_OF_IN _HPC_CALL _ACC	INTEGER	No	Indicates the total number of (interval) Ingress HPC calls accepted.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
NUM_OF_OUT_HPC_CALL_ACC	INTEGER	No	Indicates the total number of (interval) Engress HPC calls accepted.	True	
NUM_OF_HPC_4XX_MSG_SENT	INTEGER	No	Indicates the total number of (interval) sent HPC 4xx messages.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

SipIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
ZNAME	STRING	Yes	The name of the address context zone.	False	N/A
NAME	STRING	Yes	The name of this SIP trunk group.	False	N/A
SUM_RCV_INVITE	COUNTER	No	The sum of the total number of (interval) received Invite messages.	True	SUM
SUM_SND_INVITE	COUNTER	No	The sum of the total number of (interval) sent Invite messages.	True	SUM
SUM_RCV_ACK	COUNTER	No	The sum of the total number of (interval) Received Ack.	True	SUM
SUM_SND_ACK	COUNTER	No	The sum of the total number of (interval) Sent Ack messages.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_RCV_PRACK	COUNTER	No	The sum of the total number of (interval) received Prack messages.	True	SUM
SUM_SND_PRACK	COUNTER	No	The sum of the total number of (interval) sent Prack messages.	True	SUM
SUM_RCV_INFO	COUNTER	No	The sum of the total number of (interval) received INFO messages.	True	SUM
SUM_SND_INFO	COUNTER	No	The sum of the total number of (interval) sent INFO messages.	True	SUM
SUM_RCV_REFER	COUNTER	No	The sum of the total number of (interval) received Refer messages.	True	SUM
SUM_SND_REFER	COUNTER	No	The sum of the total number of (interval) sent Refer messages.	True	SUM
SUM_RCV_BYE	COUNTER	No	The sum of the total number of (interval) Received Bye messages.	True	SUM
SUM_SND_BYE	COUNTER	No	The sum of the total number of (interval) sent Bye messages.	True	SUM
SUM_RCV_CANCEL	COUNTER	No	The sum of the total number of (interval) received Cancel messages.	True	SUM
SUM_SND_CANCEL	COUNTER	No	The sum of the total number of (interval) sent Cancel messages.	True	SUM
SUM_RCV_REGISTER	COUNTER	No	The sum of the total number of (interval) received Register messages.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SND_REGISTER	COUNTER	No	The sum of the total number of (interval) sent Register messages.	True	SUM
SUM_RCV_UPDATE	COUNTER	No	The sum of the total number of (interval) received Update messages.	True	SUM
SUM_SND_UPDATE	COUNTER	No	The sum of the total number of (interval) sent Update messages.	True	SUM
SUM_RCV18_X	COUNTER	No	The sum of the total number of (interval) received 18x messages.	True	SUM
SUM_SND18_X	COUNTER	No	The sum of the total number of (interval) sent 18x messages.	True	SUM
SUM_RCV1_XX	COUNTER	No	The sum of the total number of (interval) received 1xx messages except 18x messages.	True	SUM
SUM_SND1_XX	COUNTER	No	The sum of the total number of (interval) sent 1xx messages except 18x messages.	True	SUM
SUM_RCV2_XX	COUNTER	No	The sum of the total number of (interval) received 2xx (Invite) messages.	True	SUM
SUM_SND2_XX	COUNTER	No	The sum of the total number of (interval) sent 2xx (Invite) messages.	True	SUM
SUM_RCV_NON_INV2_XX	COUNTER	No	The sum of the total number of (interval) received 2xx (Non-Invite) messages.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SND_NON_I NV2_XX	COUNTER	No	The sum of the total number of (interval) sent 2xx (Non-Invite) messages.	True	SUM
SUM_RCV3_XX	COUNTER	No	The sum of the total number of (interval) received 3xx messages.	True	SUM
SUM_SND3_XX	COUNTER	No	The sum of the total number of (interval) sent 3xx messages.	True	SUM
SUM_RCV4_XX	COUNTER	No	The sum of the total number of (interval) received 4xx messages.	True	SUM
SUM_SND4_XX	COUNTER	No	The sum of the total number of (interval) sent 4xx messages.	True	SUM
SUM_RCV5_XX	COUNTER	No	The sum of the total number of (interval) receive 5xx messages.	True	SUM
SUM_SND5_XX	COUNTER	No	The sum of the total number of (interval) sent 5xx messages.	True	SUM
SUM_RCV6_XX	COUNTER	No	The sum of the total number of (interval) receive 6xx messages.	True	SUM
SUM_SND6_XX	COUNTER	No	The sum of the total number of (interval) sent 6xx messages.	True	SUM
SUM_RCV_NON_I NV_ERR	COUNTER	No	The sum of the total number of (interval) receive Nonlvite Error messages.	True	SUM
SUM_SND_NON_I NV_ERR	COUNTER	No	The sum of the total number of (interval) sent Nonlvite Error messages.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_RCV_UNKN OWN_MSG	COUNTER	No	The sum of the total number of (interval) receive Unknown messages.	True	SUM
SUM_RCV_SUBS CRIBER	COUNTER	No	The sum of the total number of (interval) receive Subscriber messages.	True	SUM
SUM_SND_SUBS CRIBER	COUNTER	No	The sum of the total number of (interval) sent Subscriber messages.	True	SUM
SUM_RCV_NOTIF Y	COUNTER	No	The sum of the total number of (interval) receive Notify messages.	True	SUM
SUM_SND_NOTIF Y	COUNTER	No	The sum of the total number of (interval) sent Notify messages.	True	SUM
SUM_RCV_OPTIO N	COUNTER	No	The sum of the total number of (interval) receive Option messages.	True	SUM
SUM_SND_OPTIO N	COUNTER	No	The sum of the total number of (interval) sent Option messages.	True	SUM
SUM_INV_RE_TR ANSMIT	COUNTER	No	The sum of the total number of (interval) Invite messages Re-Transmitted.	True	SUM
SUM_REG_RE_T RANSMIT	COUNTER	No	The sum of the total number of (interval) Register messages Re-Transmitted.	True	SUM
SUM_BYE_RETR ANSMIT	COUNTER	No	The sum of the total number of (interval) Bye messages Re-Transmitted.	True	SUM
SUM_CANCEL_R E_TRANSMIT	COUNTER	No	The sum of the total number of (interval) Cancel messages Re-Transmitted.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_OTHER_RE_TRANSMIT	COUNTER	No	The sum of the total number of (interval) Other messages Re-Transmitted.	True	SUM
SUM_RCV_MESSAGE	COUNTER	No	The sum of the total number of (interval) received Message method.	True	SUM
SUM_SND_MESSAGE	COUNTER	No	The sum of the total number of (interval) sent Message method.	True	SUM
SUM_RCV_PUBLISH	COUNTER	No	The sum of the total number of (interval) received Publish method.	True	SUM
SUM_SND_PUBLISH	COUNTER	No	The sum of the total number of (interval) sent Publish method.	True	SUM
SUM_EMERGENCY_ACCEPT	COUNTER	No	The sum of the total number of (interval) emergency calls accepted.	True	SUM
SUM_EMERGENCY_REJECT_BWCALL	COUNTER	No	The sum of the total number of (interval) emergency calls rejected because of bandwidth limit or call limit.	True	SUM
SUM_EMERGENCY_REJECT_POLICER	COUNTER	No	The sum of the total number of (interval) emergency calls rejected because of Priority Policer.	True	SUM
SUM_HPC_ACCEPT	COUNTER	No	The sum of the total number of (interval) HPC calls accepted.	True	SUM
SUM_NUM_OF_CALLS_SENDING_AARS	COUNTER	No	The sum of the number of calls sending AAR requests.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_OF_RECEIVED_AAA_FAILURES	COUNTER	No	The sum of the number of received AAA failures.	True	SUM
SUM_NUM_OF_TOTAL_AAR_SENT	COUNTER	No	The sum of the total number of AAR messages sent.	True	SUM
SUM_NUM_OF_TIMEOUT_OR_ERROR_AAR	COUNTER	No	The sum of the number of AAR messages not answered.	True	SUM
SUM_EMERGENCY_REG_ACCEPT	COUNTER	No	The sum of the number of (interval) emergency registrations accepted.	True	SUM
SUM_EMERGENCY_REG_REJECT_LIMIT	COUNTER	No	The sum of the number of (interval) emergency registrations rejected because of the registration limit.	True	SUM
SUM_EMERGENCY_REG_REJECT_POLICER	COUNTER	No	The sum of the number of (interval) emergency registrations rejected because of the Priority Policer.	True	SUM
SUM_PARSE_ERROR	COUNTER	No	The sum of the total number of (interval) Parse Errors.	True	SUM
SUM_NUM_OF_TOTAL_UDR_SENT	COUNTER	No	The sum of the total number of UDR messages sent.	True	SUM
SUM_NUM_OF_TIMEOUT_UDR_ERROR	COUNTER	No	The sum of the number of UDR messages not answered.	True	SUM
SUM_NUM_OF_RECEIVED_UDA_SUCCESS	COUNTER	No	The sum of the number of received UDA success.	True	SUM
SUM_NUM_OF_RECEIVED_UDA_FAILURES	COUNTER	No	The sum of the number of received UDA failures.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_TOTAL_NUM_S8HR_OUT_REG	COUNTER	No	The sum of the total number (includes success and failed) of registration received from S8HR Outbound Roaming Users.	True	SUM
SUM_NUM_S8HR_OUT_REG_SUC	COUNTER	No	The sum of the number of successful registration from S8HR Outbound Roaming Users.	True	SUM
SUM_NUM_S8HR_OUT_REG_FAIL	COUNTER	No	The sum of the number of S8HR Outbound Roaming Users registrations failed.	True	SUM
SUM_TOTAL_NUM_S8HR_OT_NML_CALL	COUNTER	No	The sum of the total number of normal calls initiated from S8HR Outbound Roaming Users.	True	SUM
SUM_NUM_OF_S8HR_OT_NML_CALL_SUC	COUNTER	No	The sum of the number of successful normal calls from S8HR Outbound Roaming Users.	Tru	SUM
SUM_NUM_OF_S8HR_OT_NML_CALL_FAIL	COUNTER	No	The sum of the total number of failed normal calls from S8HR Outbound Roaming Users.	True	SUM
SUM_NUM_OF_S8HR_OT_EMG_CALL_REJ	COUNTER	No	The sum of the number of S8HR Outbound Roaming User's emergency calls rejected.	True	SUM
SUM_NUM_OF_S8HR_IN_EMG_REG_SUC	COUNTER	No	The sum of the number of Successful registration from S8HR Inbound Roaming Users.	True	SUM
SUM_NUM_OF_S8HR_IN_EMG_REG_FAIL	COUNTER	No	The sum of the number of S8HR Inbound User's registration rejected.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_OF_S8HR_IN_EMG_CALL_SUC	COUNTER	No	The sum of the number of successful emergency calls from S8HR Inbound User.	True	SUM
SUM_NUM_OF_S8HR_IN_EMG_CALL_FAIL	COUNTER	No	The sum of the number of S8HR Inbound Users emergency calls failed.	True	SUM
SUM_NUM_OF_IN_HPC_CALL_ACC	COUNTER	No	The sum of the total number of (interval) Ingress HPC calls accepted.	True	SUM
SUM_NUM_OF_OUT_HPC_CALL_ACC	COUNTER	No	The sum of the total number of (interval) Egress HPC calls accepted.	True	SUM
SUM_NUM_OF_HPC_4XX_MSG_SENT	COUNTER	No	The sum of the total number of (interval) sent HPC 4xx messages.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

SipIpPeerOptionsIntervalStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
ACNAME	STRING	Yes	The name of the address context.	False	N/A	N/A
ZNAME	STRING	Yes	The name of this Zone.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_NAME	STRING	Yes	The name of this SIP IP Peer.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_DIRECTION	STRING	Yes	Indicates the direction of the (interval) SIP Options/Response messages.	False	N/A	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
SIP_IP_PEER_OPTIONS_MESSAGE	STRING	Yes	Indicates the cause code of the (interval) SIP Options/Response messages.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_MESSAGE_COUNT	COUNTER	No	Indicates the total number of (interval) SIP Options/Response messages for the specified cause code.	True	Sum	N/A
CE_NAME	STRING	No	The name of the compute element for this entity.	False	N/A	N/A

SipIpPeerOptionsIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
ACNAME	STRING	Yes	The name of the address context.	False	N/A	N/A
ZNAME	STRING	Yes	The name of this Zone.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_NAME	STRING	Yes	The name of this SIP IP Peer.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_DIRECTION	STRING	Yes	Indicates the direction of the (interval) SIP Options/Response messages.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_MESSAGE	STRING	Yes	Indicates the cause code of the (interval) SIP Options/Response messages.	False	N/A	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
SIP_IP_PEER_OPTIONS_MSG_COUNT	COUNTER	No	Indicates the total number of (interval) SIP Options/Response messages for the specified cause code.	True	Sum	N/A
CE_NAME	STRING	No	The name of the compute element for this entity.	False	N/A	N/A

SipLocalRegistrarRegCountIntStats

Column Name	Column Type	Description	Index	canAggregate
NAME	INTEGER	The name of the system.	True	False
SIP_REG_ATTEMPT_COUNT	GAUGE	The number of SIP registration attempts	False	True
SIP_REG_CHALLENGED_COUNT	GAUGE	The current number of challenged SIP registrations	False	True
SIP_REG_FAILED_403_COUNT	GAUGE	The total number of SIP registrations failed with 403	False	True
SIP_REG_FAILED_404_COUNT	GAUGE	The total number of SIP registrations failed with 404	False	True
SIP_REG_FAILED_503_COUNT	GAUGE	The total number of SIP registrations failed with 503	False	True
SIP_REG_FAILED_OTHERS_COUNT	GAUGE	The total number of SIP registrations failed with other response codes	False	True
SIP_REG_STABLE_COUNT	GAUGE	The current number of stable SIP registrations	False	True
LICENSE_MODE (Metric column)	INTEGER	It is copy of SBX7KLicenseUsageStats.LICENSE_MODE	False	True

Column Name	Column Type	Description	Index	canAggregate
CE_NAME	STRING	The name of the compute element for this entity.	False	False

sipOcsCallIntervalStatistics

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context zone.	
NAME	STRING	Yes	The name of this SIP trunk group.	
ATTEMPTED_CALLS	GAUGE	No	Current Attempted OCS Call statistics.	
RELAYED_CALLS	GAUGE	No	Current Relayed OCS Invite to Engress side statistics.	
ESTABLISHED_CALLS	GAUGE	No	Current Established OCS Call statistics.	
SUCCESSFUL_CALLS	GAUGE	No	Current Successful OCS Call statistics.	
FAILED_CALLS	GAUGE	No	Current Failed OCS Call statistics.	
PENDING_CALL	GAUGE	No	Current Pending OCS Call statistics.	
REJECTED_CALL	GAUGE	No	Current SBX Rejected OCS Call statistics.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

SipRegCountStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
NAME	INTEGER	Yes	Name of the system.	
SIP_REG_COUNT_ATTEMPTS	COUNTER	No	Indicates the number of SIP registration attempts.	
SIP_REG_COUNT_CUM_COMPLETIONS	COUNTER	No	Indicates the accumulative number of completed SIP registration attempts.	
SIP_REG_COUNT_PENDING	COUNTER	No	Indicates the current number of pending SIP registrations.	
SIP_REG_COUNT_STABLE	COUNTER	No	Indicates the current number of stable SIP registrations.	
SIP_REG_COUNT_TOTAL	COUNTER	No	Indicates the total number of current SIP registrations.	
SIP_EMERGENCY_REG_ACCEPT_TOTAL	COUNTER	No	Indicates the total number of accepted emergency SIP registrations.	
SIP_EMERGENCY_REG_ACTIVE_TOTAL	COUNTER	No	Indicates the total number of active emergency SIP registrations.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

SipRegCountStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
NAME	INTEGER	Yes	Name of the system.	False	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SIP_REG_COUNT_ATTEMPTS	COUNTER	No	The sum of the number of SIP registration attempts.	True	SUM
SUM_SIP_REG_COUNT_CUM_COMPLETIONS	COUNTER	No	The sum of the accumulative number of completed SIP registration attempts.	True	SUM
SUM_SIP_REG_COUNT_TOTAL	COUNTER	No	The sum of the total number of current SIP registrations.	True	SUM
SUM_SIP_EMERGENCY_REG_ACCEPT_TOTAL	COUNTER	No	The sum of the total number of accepted emergency SIP registrations.	True	SUM
AVG_SIP_EMERGENCY_REG_ACTIVE_TOTAL	GUAGE	No	Indicates the total number of emergency SIP registrations currently active.	True	MEAN
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

SipSigConnStatisticsStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	N/A
ZNAME	STRING	Yes	The name of the address context zone.	
IND	GAUGE	Yes	The index of this SIP Signaling Port.	
TCP_CONNECTION	COUNTER	No	Number of current TCP connections	
TOTAL_TCP_CONNECTION	COUNTER	No	Number of total TCP connections made.	

Column Name	Column Type	Index	Description	CLI Command Reference
ACTIVE_TLS_TCP_CONNECTION	COUNTER	No	Number of current TLS-TCP connections made.	
TOTAL_TLS_TCP_CONNECTION	COUNTER	No	Number of total TLS-TCP connections.	
CE_NAME	STRING	No	The name of the compute element for this entry	

SipSigPortStatisticsStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context zone.	
IND	GAUGE	Yes	The index of this SIP Signaling Port.	
CALL_RATE	INTEGER	No	Number of SIP calls per second during the last minute.	
ORIG_CALLS	INTEGER	No	Total number of outgoing calls sent out from this signaling port.	
TERM_CALLS	INTEGER	No	Total number of incoming calls received on this signaling port.	
TX_PDUS	COUNTER64	No	The total number of signaling PDUS sent out on this port.	
RX_PDUS	COUNTER64	No	The total number of signaling PDUS received on this port.	

Column Name	Column Type	Index	Description	CLI Command Reference
TX_BYTES	COUNTER64	No	The total number of signaling BYTES sent out from this port.	
RX_BYTES	COUNTER64	No	The total number of signaling BYTES received by this port.	
IN_REGS	INTEGER	No	Total number of inbound registration(s) received on this signaling port.	
OUT_REGS	INTEGER	No	Total number of outbound registration(s) sent on this signaling port.	
TX500S	INTEGER	No	The total number of 500 responses generated by the SLB when it is unable to forward a request.	
TX503S	INTEGER	No	The total number of 503 responses generated by the SLB when there are no backend SBCs able to handle the request due to the congestion or the cac restrictions.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

SipSigPortStatisticsStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
ZNAME	STRING	Yes	The name of the address context zone.	False	N/A
IND	GAUGE	Yes	The index of this SIP Signaling Port.	False	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_CALL_RATE	INTEGER	No	The average of the count of SIP calls per second during the last minute.	True	AVG
SUM_CALL_RATE	INTEGER	No	The sum of the count of SIP calls per second during the last minute.	True	SUM
AVG_ORIG_CALLS	INTEGER	No	The average of the count of outgoing calls sent out from this signaling port.	True	AVG
SUM_ORIG_CALLS	INTEGER	No	The sum of the count of outgoing calls sent out from this signaling port.	True	SUM
AVG_TERM_CALLS	INTEGER	No	The average of the count of incoming calls received on this signaling port.	True	AVG
SUM_TERM_CALLS	INTEGER	No	The sum of the count of incoming calls received on this signaling port.	True	SUM
AVG_TX_PDUS	INTEGER	No	The average of the count of signaling PDUS sent out on this port.	True	AVG
SUM_TX_PDUS	INTEGER	No	The average of the count of signaling PDUS sent out on this port.	True	SUM
AVG_RX_PDUS	INTEGER	No	The average of the count of signaling PDUS received on this port.	True	AVG
SUM_RX_PDUS	INTEGER	No	The sum of the count of signaling PDUS received on this port.	True	SUM
AVG_TX_BYTES	INTEGER	No	The average of the count of signaling BYTES sent out from this port.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_TX_BYTES	INTEGER	No	The sum of the count of signaling BYTES sent out from this port.	True	SUM
AVG_RX_BYTES	INTEGER	No	The average of the count of signaling BYTES received by this port.	True	AVG
SUM_RX_BYTES	INTEGER	No	The sum of the count of signaling BYTES received by this port.	True	SUM
AVG_IN_REGS	INTEGER	No	The average of the count of inbound registration(s) received on this signaling port.	True	AVG
SUM_IN_REGS	INTEGER	No	The sum of the count of inbound registration(s) received on this signaling port.	True	SUM
AVG_OUT_REGS	INTEGER	No	The average of the count of outbound registration(s) sent on this signaling port.	True	AVG
SUM_OUT_REGS	INTEGER	No	The sum of the count of outbound registration(s) sent on this signaling port.	True	SUM
MEAN_TX500S	INTEGER	No	The total number of 500 responses generated by the SLB when it is unable to forward a request.	True	MEAN
MEAN_TX503S	INTEGER	No	The total number of 503 responses generated by the SLB when there are no backend SBCs able to handle the request due to the congestion or the cac restrictions.	True	MEAN
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

SipSigPortTlsStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	NA
ZNAME	STRING	Yes	The name of the address context zone.	
IND	GAUGE	Yes	The index of this SIP Signaling Port.	
CURRENT_CLIENT_SESSIONS	INTEGER	No	Number of client sessions currently active.	
CURRENT_SERVER_SESSIONS	INTEGER	No	Number of server sessions currently active.	
CURRENT_SUSPENDED_SESSIONS	INTEGER	No	Number of server sessions currently suspended.	
TOTAL_CLIENT_SESSIONS	INTEGER	No	Cumulative total number of client sessions.	
TOTAL_SERVER_SESSIONS	INTEGER	No	Cumulative total number of server sessions.	
CURRENT_CLIENT_HANDSHAKES	INTEGER	No	Number of incomplete client handshakes.	
CURRENT_SERVER_HANDSHAKES	INTEGER	No	Number of incomplete server handshakes.	
SESSION_RESUMPTIONS	INTEGER	No	Number of resumed server sessions.	
NO_CIPHER_SUITE	INTEGER	No	Number of handshake failures due to inability to converge on a cipher suite.	
HANDSHAKE_TIMEOUTS	INTEGER	No	Number of handshakes that timed out before completing.	

Column Name	Column Type	Index	Description	CLI Command Reference
HIGHER_AUTH_TIMEOUT	INTEGER	No	Number of handshakes in which the SBC was the server and the client did not authenticate itself through TLS and failed to authenticate itself through any higher level protocol (for example, SIP) before timing out.	
CLIENT_AUTH_FAILURES	INTEGER	No	Number of times peer failed TLS authentication with SBC as the client.	
SERVER_AUTH_FAILURES	INTEGER	No	Number of times peer failed TLS authentication with SBC as the server.	
FATEL_ALERTS_RECEIVED	INTEGER	No	Number of FATAL Alerts received.	
WARNING_ALERTS_RECEIVED	INTEGER	No	Number of WARNING Alerts received.	
HANDSHAKE_FAILURES	INTEGER	No	Cumulative total of all handshake failures.	
RECEIVE_FAILURES	INTEGER	No	Number of receive failures (failure to decrypt).	
SEND_FAILURES	INTEGER	No	Number of send failures (failure to encrypt).	
NO_AUTH_DROPS	INTEGER	No	Number of SIP messages dropped due to lack of peer authentication at the SIP level.	
NO_AUTH488	INTEGER	No	Number of SIP messages rejected with 488 due to lack of peer authentication at the SIP level.	

Column Name	Column Type	Index	Description	CLI Command Reference
MID_CONNECTION_HELLO	INTEGER	No	Number times a peer sent a TLS Hello on a connection that was already up (that is, the peer tried to renegotiate.).	
NO_CLIENT_CERT	INTEGER	No	Number times we were the client and we failed to derive a certificate to send the server.	
VALIDATION_FAILURES	INTEGER	No	Number of failed certificate validations.	
CURRENT_CLIENT_CONNECTIONS	INTEGER	No	Current number of client tls connections.	
TOTAL_CLIENT_CONNECTIONS	INTEGER	No	Cumulative total number of client tls connections.	
CURRENT_SERVER_CONNECTIONS	INTEGER	No	Current number of server tls connections.	
TOTAL_SERVER_CONNECTIONS	INTEGER	No	Cumulative total number of server tls connections.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

Note

CURRENT_CLIENT_SESSIONS, CURRENT_SUSPENDED_SESSIONS, TOTAL_CLIENT_SESSIONS are not valid for SBC 4.0 and higher versions.

SipSubCountStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
NAME	INTEGER	Yes	Name of the system.	False	
SIP_SUB_COUNT_ATTEMPTS	COUNTER	No	Indicates the number of SIP relayed subscription attempts.	True	
SIP_SUB_COUNT_CUM_COMPLETIONS	COUNTER	No	Indicates the accumulative number of completed SIP subscription attempts.	True	
SIP_SUB_COUNT_STABLE	COUNTER	No	Indicates the current number of stable SIP subscription.	True	
SIP_SUB_COUNT_TOTAL	COUNTER	No	Indicates the total number of current SIP subscription on this card (SIP_SUB_COUNT_ATTEMPTS + SIP_SUB_COUNT_CUM_COMPLETIONS)	True	
SIP_SUB_COUNT_FAILURE	COUNTER	No	Indicates the number of SIP relayed subscription failures.	False	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

SipSubCountStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type (SUM/AVG)
ACNAME	STRING	Yes	The name of the address context.	False	N/A
NAME	INTEGER	Yes	Name of the system.	False	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type (SUM/AVG)
SUM_SIP_SUB_COUNT_ATTEMPTS	COUNTER	No	The sum of the number of SIP relayed subscription attempts.	True	SUM
SUM_SIP_SUB_COUNT_CUM_COMPLETIONS	COUNTER	No	The sum of the accumulative number of completed SIP subscription attempts.	True	SUM
AVG_SIP_SUB_COUNT_STABLE	GAUGE	No	The current number of stable SIP subscription on this card.	True	MEAN
SIP_SUB_COUNT_FAILURE	COUNTER	No	Indicates the number of SIP relayed subscription failures.	False	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

SipTrunkGroupOptionsIntervalStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
ACNAME	STRING	Yes	The name of the address context.	False	N/A	No
ZNAME	STRING	Yes	The name of this zone.	False	N/A	No
SIP_TG_OPTIONS_NAME	STRING	Yes	The name of this SIP trunk group.	False	N/A	No
SIP_TG_OPTIONS_DIRECTION	STRING	Yes	The direction of the (interval) SIP Options/Response messages.	False	N/A	No
SIP_TG_OPTIONS_MESSAGE	STRING	Yes	The cause code of the (interval) SIP Options/Response messages.	False	N/A	No

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
SIP_TG_OPTIONS_MSG_COUNT	COUNTER	No	The total number of (interval) SIP Options/Response messages for the specified cause code.	True	SUM	No
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A	No

SipTrunkGroupOptionsIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
ACNAME	STRING	Yes	The name of the address context.	False	N/A	No
ZNAME	STRING	Yes	The name of this zone.	False	N/A	No
SIP_TG_OPTIONS_NAME	STRING	Yes	The name of this SIP trunk group.	False	N/A	No
SIP_TG_OPTIONS_DIRECTION	STRING	Yes	The direction of the (interval) SIP Options/Response messages.	False	N/A	No
SIP_TG_OPTIONS_MESSAGE	STRING	Yes	The cause code of the (interval) SIP Options/Response messages.	False	N/A	No
SIP_TG_OPTIONS_MSG_COUNT	COUNTER	No	The total number of (interval) SIP Options/Response messages for the specified cause code.	True	SUM	No
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A	No

Sys Stats

SysCongestionIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_LEVEL_MC 1_COUNT	COUNTER	No	The current number of transitions into MC1.	True	SUM
SUM_LEVEL_MC 1_TOTAL_TIME	COUNTER	No	The current sum of time spent in MC1.	True	SUM
SUM_LEVEL_MC 2_COUNT	COUNTER	No	The current number of transitions into MC2.	True	SUM
SUM_LEVEL_MC 2_TOTAL_TIME	COUNTER	No	The current sum of time spent in MC2.	True	SUM
SUM_LEVEL_MC 3_COUNT	COUNTER	No	The current number of transitions into MC3.	True	SUM
SUM_LEVEL_MC 3_TOTAL_TIME	COUNTER	No	The current sum of time spent in MC3.	True	SUM
SUM_OVERLOAD _REJECTS	COUNTER	No	The current number of calls rejected due to the system congestion.	True	SUM
AVG_AVG_CALL_ RATE	GAUGE	No	The current system average call arrival rate.	True	MEAN
AVG_PEAK_CALL_ RATE	GAUGE	No	The current system peak call arrival rate.	True	MEAN
SUM_CALL_ARRI VALS	COUNTER	No	The current number of call arrivals.	True	SUM
SUM_EMERGEN CY_CALL_ARRIV ALS	COUNTER	No	The current number of SIP emergency calls arrived.	True	SUM
SUM_EMERGEN CY_CALL_REJEC TS	COUNTER	No	The sum of SIP emergency calls count rejected for the specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SIP_REG_ARRIVALS	COUNTER	No	The current number of SIP registrations arrived.	True	SUM
SUM_SIP_REG_REJECTS	COUNTER	No	The current number of SIP registrations rejected.	True	SUM
AVG_AVG_REG_RATE	GAUGE	No	The current average SIP registration arrival rate.	True	MEAN
AVG_PEAK_REG_RATE	GAUGE	No	The current peak SIP registration arrival rate.	True	MEAN
AVG_MAX_ACTIVE_CALLS	GAUGE	No	High water mark of the total number of active calls in current interval for system level.	True	MEAN
AVG_SIP_SUBS_ARRIVALS	GAUGE	No	The current number of SIP subscribes arrived.	True	MEAN
AVG_SIP_SUBS_REJECTS	GAUGE	No	The current number of SIP subscribes rejected.	True	MEAN
AVG_AVG_SUBS_RATE	GAUGE	No	The current average SIP subscribe arrival rate.	True	MEAN
AVG_PEAK_SUBS_RATE	GAUGE	No	The current peak SIP subscribe arrival rate.	True	MEAN
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

SysCpuUtilIntStatsSts

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	This object indicates the configured CE name.	Show Status System
CPU	GAUGE	Yes	The CPU number.	
AVERAGE	GAUGE	No	The average CPU percentage utilization for this interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
HIGH	GAUGE	No	The high CPU percentage utilization for this interval.	
LOW	GAUGE	No	The low CPU percentage utilization for this interval.	

SysMemoryUtilIntStatsSts

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	This object indicates the configured CE name.	Show Status System
AVERAGE	GAUGE	No	The average memory percentage utilization for this interval.	
HIGH	GAUGE	No	The high memory percentage utilization for this interval.	
LOW	GAUGE	No	The low memory percentage utilization for this interval.	
AVERAGE_SWAP	GAUGE	No	The average swap memory percentage utilization for this interval.	
HIGH_SWAP	GAUGE	No	The high swap memory percentage utilization for this interval.	
LOW_SWAP	GAUGE	No	The low swap memory percentage utilization for this interval.	

SystemCongestionIntervalStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
NAME	INTEGER	Yes	Name of the system.	False	Show Status System

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
LEVEL_MC1_COUNT	COUNTER	No	The number of transitions into MC1 for the specified interval.	False	
LEVEL_MC1_TOTAL_TIME	COUNTER	No	The sum of time spent in MC1 for the specified interval.	False	
LEVEL_MC2_COUNT	COUNTER	No	The number of transitions into MC2 for the specified interval.	False	
LEVEL_MC2_TOTAL_TIME	COUNTER	No	The sum of time spent in MC2 for the specified interval.	False	
LEVEL_MC3_COUNT	COUNTER	No	The number of transitions into MC3 for the specified interval.	False	
LEVEL_MC3_TOTAL_TIME	COUNTER	No	The sum of time spent in MC3 for the specified interval.	False	
OVERLOAD_REJECTS	COUNTER	No	The number of calls rejected due to System congestion for the specified interval.	False	
AVG_CALL_RATE	GAUGE	No	The system average call arrival rate for the specified interval.	False	
PEAK_CALL_RATE	GAUGE	No	The system peak call arrival rate for the specified interval.	False	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
CALL_ARRIVALS	COUNTER	No	The number of call arrivals for the specified interval.	False	
EMERGENCY_CALL_ARRIVALS	COUNTER	No	The number of SIP emergency calls arrived for the specified interval.	False	
EMERGENCY_CALL_REJECTS	COUNTER	No	The number of SIP emergency calls arrived for the specified interval.	False	
SIP_REG_ARRIVALS	COUNTER	No	The number of SIP registrations arrived for the specified interval.	False	
SIP_REG_REJECTS	COUNTER	No	The number of SIP registrations rejected for the specified interval.	False	
AVG_REG_RATE	GAUGE	No	The average SIP registration arrival rate for the specified interval.	False	
PEAK_REG_RATE	GAUGE	No	The peak SIP registration arrival rate for the specified interval.	False	
MAX_ACTIVE_CALLS	GAUGE	No	High watermark of the total number of active calls in current interval for system level.	True	
SIP_SUBS_ARRIVALS	GAUGE	No	The current number of SIP subscribes arrived.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SIP_SUBS_REJECTS	GAUGE	No	The current number of SIP subscribes rejected.	True	
AVG_SUBS_RATE	GAUGE	No	The current average SIP subscribe arrival rate.	True	
PEAK_SUBS_RATE	GAUGE	No	The current peak SIP subscribe arrival rate.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

SystemLicenseInfoStats

Note

SystemLicenseInfoStats is available only if SBC 3.1 Device Manager is installed.

Column Name	Column Type	Index	Description	CLI Command Reference
FEATURE_NAME	STRING	Yes	This object indicates the feature name.	Show Table System
LICENSE_ID	STRING	Yes	This object indicates the license Id.	
EXPIRATION_DATE	STRING	No	This object indicates the license expiry date for a feature.	
USAGE_LIMIT	INTEGER	No	This object indicates the usage limit of a feature.	
SOURCE	STRING	No	This object indicates where the licenses is located, nodeLocked or domain.	

Column Name	Column Type	Index	Description	CLI Command Reference
IN_USE	GAUGE	No	This object indicates the number of licenses used by the application.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

TcpGeneralGroupStats

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	The name of the compute element for this entry.	NA
ESTABLISHED_CONNECTIONS	GAUGE	No	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT. (currEstab)	
CLIENT_CONNECTIONS	COUNTER	No	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state. (activeOpens)	
SERVER_CONNECTIONS	COUNTER	No	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state. (passiveOpens)	
FAILED_ATTEMPTS	COUNTER	No	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state. (attemptFails)	

Column Name	Column Type	Index	Description	CLI Command Reference
IN_SEGMENTS	COUNTER	No	The total number of segments received, including those received in error. This count includes segments received on currently established connections.	
OUT_SEGMENT S	COUNTER	No	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.	
RETRANS_SEG MENTS	COUNTER	No	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.	
IN_ERRORS	COUNTER	No	The total number of segments received in error (for example, bad TCP checksums).	
IN_RESETS	COUNTER	No	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state. (estabResets)	
OUT_RESETS	COUNTER	No	The number of TCP segments sent containing the RST flag.	

TrafficControlStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context

Column Name	Column Type	Index	Description	CLI Command Reference
ZNAME	STRING	Yes	The name of the address context zone.	
NAME	STRING	Yes	The name of this trunk group.	
SILC	GAUGE	No	The number of calls cancelled due to SILC for this trunk group for the specified interval.	
STR_CANT	GAUGE	No	The number of calls cancelled due to STR for this trunk group for the specified interval.	
STR_SKIP	GAUGE	No	The number of calls skipped due to STR for this trunk group for the specified interval.	
SKIP	GAUGE	No	The number calls skipped due to the SKIP traffic control for this trunk group for the specified interval.	
CANT	GAUGE	No	The number of calls cancelled due to CANT for this trunk group for the specified interval.	
CANF	GAUGE	No	The number of calls cancelled due to CANF for this trunk group for the specified interval.	
ACC_CANT	GAUGE	No	The number of calls cancelled due to ACC for this trunk group for the specified interval.	
ACC_SKIP	GAUGE	No	The number of calls skipped due to ACC for this trunk group for the specified interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
ROUTE_ATTEMPTS_IRR	GAUGE	No	The number of reroute attempts due to IRR for this trunk group for the specified interval.	
ROUTE_ATTEMPTS_SIRR	GAUGE	No	The number of reroute attempts due to SIRR for this trunk group for the specified interval.	
ROUTE_ATTEMPTS_ORR	GAUGE	No	The number of reroute attempts due to ORR for this trunk group for the specified interval.	
ROUTE_ATTEMPTS_SORR	GAUGE	No	The number of reroute attempts due to SORR for this trunk group for the specified interval.	
SUCCESSFUL_IRR	GAUGE	No	The number of successful reroutes due to IRR for this trunk group for the specified interval.	
SUCCESSFUL_SIRR	GAUGE	No	The number of successful reroutes due to SIRR for this trunk group for the specified interval.	
SUCCESSFUL_ORR	GAUGE	No	The number of successful reroutes due to ORR for this trunk group for the specified interval.	
SUCCESSFUL_SORR	GAUGE	No	The number of successful reroutes due to SORR for this trunk group for the specified interval.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

UdpGeneralGroupStats

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	The name of the compute element for this entry.	Show Table Address Context
IN_DATAGRAMS	COUNTER	No	The total number of UDP datagrams delivered to UDP users.	
OUT_DATAGRAMS	COUNTER	No	The total number of UDP datagrams sent from this entity.	
UNKNOWN_PORTS	COUNTER	No	The total number of received UDP datagrams for which there was no application at the destination port.	
IN_ERRORS	COUNTER	No	The number of received UDP datagrams that this entity cannot deliver for reasons other than the lack of an application at the destination port.	

ZoneIntervalStatisticsStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context
NAME	STRING	Yes	The name of this zone.	False	
INGRESS_FAIL_CALL_LIMIT	COUNTER	No	Number of incoming calls failed due to Call Limit check on Zone.	False	
EGRESS_FAIL_CALL_LIMIT	COUNTER	No	Number of outgoing calls failed due to Call Limit check on Zone.	False	
INGRESS_FAIL_CALL_POLICING	COUNTER	No	Number of incoming calls failed due to Call Policer check on Zone.	False	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
EGRESS_FAIL_CALL_POLICING	COUNTER	No	Number of outgoing calls failed due to Call Policer check on Zone.	False	
INGRESS_FAIL_BWLIMIT	COUNTER	No	Number of incoming calls failed due to Bandwidth Limit check on Zone.	False	
EGRESS_FAIL_BWLIMIT	COUNTER	No	Number of outgoing calls failed due to Bandwidth Limit check on Zone.	False	
INGRESS_SIP_REG_FAIL_LIMIT	COUNTER	No	Number of incoming SIP Registrations failed due to Registrations Limit check on Zone.	False	
EGRESS_SIP_REG_FAIL_LIMIT	COUNTER	No	Number of outgoing SIP Registrations failed due to Registrations Limit check on Zone.	False	
INGRESS_SIP_REG_POLICING	COUNTER	No	Number of incoming SIP Registrations failed due to ingress Policer check on Zone.	False	
EGRESS_SIP_REG_POLICING	COUNTER	No	Number of outgoing SIP Registrations failed due to egress Policer check on Zone.	False	
VIDEO_THRESHOLD_LIMIT	COUNTER	No	The number of exceeded video threshold limits for this zone.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

ZoneIntervalStatisticsStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
NAME	STRING	Yes	The name of this zone.	False	N/A
SUM_INGRESS_F AIL_CALL_LIMIT	COUNTER	No	The sum of the number of incoming calls failed due to Call Limit check on Zone.	True	SUM
SUM_EGRESS_F AIL_CALL_LIMIT	COUNTER	No	The sum of the number of outgoing calls failed due to Call Limit check on Zone.	True	SUM
SUM_INGRESS_F AIL_CALL_POLICI NG	COUNTER	No	The sum of the number of incoming calls failed due to Call Policer check on Zone.	True	SUM
SUM_EGRESS_F AIL_CALL_POLICI NG	COUNTER	No	The sum of the number of outgoing calls failed due to Call Policer check on Zone.	True	SUM
SUM_INGRESS_F AIL_BWLIMIT	COUNTER	No	The sum of the number of incoming calls failed due to Bandwidth Limit check on Zone.	True	SUM
SUM_EGRESS_F AIL_BWLIMIT	COUNTER	No	The sum of the number of outgoing calls failed due to Bandwidth Limit check on Zone.	True	SUM
SUM_INGRESS_S IP_REG_FAIL_LIM IT	COUNTER	No	The sum of the number of incoming SIP Registrations failed due to Registrations Limit check on Zone.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_EGRESS_SIP_REG_FAIL_LIMIT	COUNTER	No	The sum of the number of outgoing SIP Registrations failed due to Registrations Limit check on Zone.	True	SUM
SUM_INGRESS_SIP_REG_POLICING	COUNTER	No	The sum of the number of incoming SIP Registrations failed due to ingress Policer check on Zone.	True	SUM
SUM_EGRESS_SIP_REG_POLICING	COUNTER	No	The sum of the number of outgoing SIP Registrations failed due to egress Policer check on Zone.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

SBC 7000 Statistics

In this section:

- [Call Stats](#)
 - [CallCountIntervalStats](#)
 - [CallFailIntervalStats](#)
 - [CallIntervalStats](#)
 - [NBS5200CallCountStats](#)
 - [DiamNodeRfIntervalStatistics](#)
 - [DnsGroupDnsServerStats](#)
- [DSP Stats](#)
 - [DspResDspCallIntervalStats](#)
 - [DspResDspUsageIntervalStats](#)
 - [EthernetPortMgmtStats](#)
 - [EthernetPortPacketStats](#)
 - [H323SigPortStatisticsStats](#)
 - [IcmpGeneralGroupStats](#)
- [IP Stats](#)
 - [IpAclOverallStats](#)
 - [IpAclRuleStats](#)
 - [IpGeneralGroupStats](#)
 - [IpPolicingSystemIntStats](#)
- [Link Stats](#)
 - [LinkDetectionGroupStats](#)
 - [LinkMonitorStats](#)
 - [SipLocalRegistrarRegCountIntStats](#)

- NBS5200TrunkGroupStatusStats
- RelayIntervalStatistics
- SBCORE Stats
 - SBCCOREFacBlockingStats
 - SBCCOREFacTotBlockStats
 - SBCCOREOodMessageIntStats
 - SBCCORESipIPPresIntStats
 - SBCCORESipRegCountDomIntStats
 - SBCCORESipTgCSSRIntStats
 - SBCCORESipTGResIntStats
 - SBCCORETGAggregatedStats
- SBX5K Stats
 - SBX5KAclOffListIntStats
 - SBX5KAggregateOffIntStats
 - SBX5KArpOffListIntStats
 - SBX5KBadEtherIpHdrOffIntStats
 - SBX5KDiscardRuleOffIntStats
 - SBX5KDtlsSrtpStats
 - SBX5KEthernetPortPacketPortStatus
 - SBX5KIpSecDecryptOffIntStats
 - SBX5KLicenseUsageStats
 - SBX5KMediaOffIntStats
 - SBX5KMtrmConnPortPeerStats
 - SBX5KRogueMediaIntStats
 - SBX5KSipByeResponseIntervalStats
 - SBX5KSipInviteResponseIntervalStats
 - SBX5KSipIpPeerIntervalStats
 - SBX5KSipOptResponseIntervalStats
 - SBX5KSipRegResponseIntervalStats
 - SBX5KSrtpDecryptOffIntStat
 - SBX5KSystemDspStatusDspUsageStats
 - SBX5KUflowOffListIntStats
- Shared CAC Stats
 - SharedCacFailureIntStats
 - SharedCacIntervalStatistics
- SIP Stats
 - SipIntervalStats
 - sipOcsCallIntervalStatistics
 - SipIpPeerOptionsIntervalStats
 - SipRegCountStats
 - SipSigConnStatisticsStats
 - SipSigPortStatisticsStats
 - SipSigPortTlsStats
 - SipSubCountStats
 - SipTrunkGroupOptionsIntervalStats
- Sys Stats
 - SysCpuUtilIntStatsSts
 - SysMemoryUtilIntStatsSts
 - SystemCongestionIntervalStats
 - SystemLicenseInfoStats
 - TcpGeneralGroupStats
 - TrafficControlStats

- [UdpGeneralGroupStats](#)
- [ZoneIntervalStatisticsStats](#)

Note

- SBX7K is considered as a subtype now. Hence, the names of all the statistics are same as SBX5K. To get the exported file names in the SBX7K format, enable **Use Sub Type in file name** and **Use Sub Type in exported SBX7K file names** in [Configure Performance Management Export Options](#). For example, the earlier exported file name used to be: SBC7KSystemDspStatusDspUsageStats. The new file name is SBX5KSystemDspStatusDspUsageStats.
- The statistics tables names are listed in the following format
<name of the table in the exported CSV file>/<name of the table in the Ribbon Application Management Platform (RAMP) PM profile>
- If the table name is same in the exported CSV file and the RAMP PM profile, it is listed only once.

Call Stats

CallCountIntervalStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
NAME	INTEGER	True	Adds a dummy key to non-config scalar element container, even though only one row is allowed in container. Without the key, tailf treats the container non-dynamic and calls get_elem per leaf instead of calling get_object per row.	True	
MAX_SESSION_COUNT	COUNTER	False	Displayed as maxSessionCallCount. The high watermark of total number of calls for the specified interval. This statistic accounts for calls that are stable.	True	
MAX_POL_RTU_COUNT	INTEGER	False	Displays the same count as MAX_SESSION_COUNT if SBC is using SBC-POL-RTU license. If SBC is not using SBC-POL-RTU license, the count is displayed as 0.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ENCRYPT_COUNT	COUNTER	False	Displayed as system wide total encrypt Call Count. The high watermark of total number of encrypt calls for the specified interval.	True	
SRTP_COUNT	COUNTER	False	Displayed as system wide total Secure Real-time Transport Protocol (SRTP) Call Count; The high watermark of total number of SRTP calls for the specified interval.	True	
VIDEO_COUNT	COUNTER	False	Displayed as system wide total video Call Count; The high watermark of total number of video calls for the specified interval.	True	
AMRNB_COUNT	COUNTER	False	The high watermark of total number of Adaptive Multi-Rate Narrowband (AMRNB) calls for the specified interval.	True	
AMRWB_COUNT	COUNTER	False	The high watermark of total number of Adaptive Multi-Rate Wideband (AMRWB) calls for the specified interval.	True	
EVRC_COUNT	COUNTER	False	The high watermark of total number of Enhanced Variable Rate Codec (EVRC) calls for the specified interval.	True	
NICEREC_COUNT	COUNTER	False	The current high watermark of total number of NICE recording calls.	True	
MRFSESS_COUNT	COUNTER	False	The current high watermark of total number of Media Resource Function (MRF) calls.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
MAX_PSX_RTU_COUNT	INTEGER	False	Displays MAX_SESSION_COUNT when SBC is using SBC-PSX-RTU license. If SBC is not using SBC-PSX-RTU license it displays the count as 0.	True	
VDSPRTU_COUNT	COUNTER	False	The high watermark of total number of trans-coded sessions for the specified interval.	True	
PDCS_COUNT	COUNTER	False	The high watermark of total number of pdcs header sessions for the specified interval.	True	
SIPREC_COUNT	COUNTER	False	The current high watermark of total number of sip recording calls.	True	
LI_ENABLED	INTEGER	False	Set based on whether LI license is available at the SBC.	True	
DSPG722_ENABLED	INTEGER	False	Set based on whether DspG722 license is available at the SBC.	True	
GMP4X1_ENABLED	INTEGER	False	Set based on whether 4X1GMP license is available at the SBC.	True	
SIPI_ENABLED	INTEGER	False	Set based on whether Sipl license is available at the SBC.	True	
SIP323_ENABLED	INTEGER	False	Set based on whether SipRec license is available at the SBC.	True	
GMP1X10_ENABLED	INTEGER	False	Set based on whether 1X10GMP license is available at the SBC.	True	
CAPACITY_ENABLED	INTEGER	False	Set based on whether Capacity license is available at the SBC.	True	
E911_ENABLED	INTEGER	False	Set based on whether E911 license is available at the SBC.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ENUM_ENABLED	INTEGER	False	Set based on whether ENUM license is available at the SBC.	True	
SWINSTANCE_ENABLED	INTEGER	False	Set based on whether Swe Instance license is available at the SBC.	True	
EVS_COUNT	COUNT	False	The high watermark of total number of Enhanced Voice Services (EVS) calls for the specified interval.	True	
SILK_COUNT	COUNT	False	The high watermark of total number of SILK Codec Transcode calls for the specified interval.	True	
SBCRCS_COUNT	COUNT	False	The high watermark of total number of OOD calls that use an RCS based service for the specified interval.	True	
SLBSESS_COUNT	COUNT	False	Displayed as system wide total stable SLB sessions Count. The high watermark of the total number of active calls for the reporting interval.	True	
LBINSTANCE_ENABLED	INTEGER	False	Set based on whether SLB license is available at the SLB.	False	
HPC_QUEUE_ATTEMPT	COUNT	False	The number of HPC calls successfully placed on HPC Call Queuing queues for the reporting interval.	True	
HPC_QUEUE_OVERFLOW	COUNT	False	The number of HPC calls which experienced unsuccessful call queuing attempts due to full queues for the reporting interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
HPC_QUE_ABANDON	COUNT	False	The number of queued HPC calls abandoned before call completion during the reporting interval.	True	
HPC_QUE_TIMEOUTS	COUNT	False	The number of HPC calls removed from the queue due to expiration of the queue timeout timer for the reporting interval.	True	
HPC_CTL_TFC_EXEM	COUNT	False	The HPC traffic control exemptions for this reporting interval.	True	
SOSBC_RT_U_COUNT	COUNTER	False	The system wide total stable SOSBC sessions count. The high water mark of total number of active calls for the reporting interval.	True	
WEB_SOCKET_COUNT	COUNTER	False	The high water mark of total number of web socket calls for this reporting interval.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

CallFailIntervalStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context zone.	
NAME	STRING	Yes	The name of this trunk group.	
IN_CALL_FAIL_NO_ROUTES	COUNTER	No	Number of inbound failed calls because there was no route available for this trunk group for the specified interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
IN_CALL_FAIL_NO_RESOURCE_S	COUNTER	No	Number of inbound failed calls because there was an unavailable resource for this trunk group for the specified interval.	
IN_CALL_FAIL_NO_SERVICE	COUNTER	No	Number of inbound failed calls because there was an unavailable service for this trunk group for the specified interval.	
IN_CALL_FAIL_INVALID_CALL	COUNTER	No	Number of inbound failed calls because there was an invalid call attempt for this trunk group for the specified interval.	
IN_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	Number of inbound failed calls because there was a network failure for this trunk group for the specified interval.	
IN_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	Number of inbound failed calls because there was a protocol error for this trunk group for the specified interval.	
IN_CALL_FAIL_UNSPECIFIED	COUNTER	No	Number of inbound failed calls for an unspecified reason for this trunk group for the specified interval.	
OUT_CALL_FAIL_NO_ROUTES	COUNTER	No	Number of outbound failed calls due to no route available for this trunk group for the specified interval.	
OUT_CALL_FAIL_NO_RESOURCES	COUNTER	No	Number of outbound failed calls due to unavailable resource for this trunk group for the specified interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
OUT_CALL_FAIL_NO_SERVICE	COUNTER	No	Number of outbound failed calls due to unavailable service for this trunk group for the specified interval.	
OUT_CALL_FAIL_INVALID_CALL	COUNTER	No	Number of outbound failed calls due to invalid call attempt for this trunk group for the specified interval.	
OUT_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	Number of outbound failed calls due to network failure for this trunk group for the specified interval.	
OUT_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	Number of outbound failed calls due to protocol error for this trunk group for the specified interval.	
OUT_CALL_FAIL_UNSPECIFIED	COUNTER	No	Number of outbound failed calls for an unspecified reason for this trunk group for the specified interval.	
ROUTING_FAILURES_RESV	COUNTER	No	Number of routing failures due to all circuits reserved for this trunk group for specified interval.	
ALLOC_FAIL_BANDWIDTH_LIMIT	COUNTER	No	Number of bandwidth Requests which fail because the specified interval of this trunk group exceeds the configured bandwidth limit.	
ALLOC_FAIL_CALL_LIMIT	COUNTER	No	Number of bandwidth Requests which fail because the specified interval of this trunk group exceeds the configured call limit.	

Column Name	Column Type	Index	Description	CLI Command Reference
NO_PSX_ROUTE	COUNTER	No	Number of failed calls on an ingress trunk group due to no routes returned from the ERE for the specified interval.	
CALL_ABANDONED	COUNTER	No	Number of calls on a toll-free TG that were abandoned while dialing for the specified interval.	
CALL_FAIL_POLICING	COUNTER	No	Number of calls on a trunk group that failed due to policing for the specified interval.	
SIP_REG_FAIL_POLICING	COUNTER	No	Number SIP registration attempts that failed due to policing on TG for specified interval.	
SIP_REG_FAIL_INTERNAL	COUNTER	No	Number SIP registration attempts that failed due to other reasons (signaling failures, and so on) on a trunk group for the specified interval.	
SIP_REG_FAIL_OTHER	COUNTER	No	The current number SIP registration attempts that failed due to other reasons (signaling failures, and so on) on a trunk group for the specified interval.	
SECURITY_FAIL	COUNTER	No	Number of calls that failed due to mismatch between the peer security and route packet service profile security on trunk group for specified interval.	
NON_REG_CALLS_FAILED	COUNTER	No	Number of failed calls due to registration requirement for SIP trunk group for the specified interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NON_MATCH_SRC_IP_CALLS_FAIL	COUNTER	No	Number of calls that failed due to mismatched source IP of IAD according to its RCB for the specified interval.	
INVALID_SPCALLS_FAILED	COUNTER	No	Number of failed calls due to mismatched ingress signaling port from CP according to RCB for the specified interval.	
SIP_SUBS_FAIL_POLICING	COUNTER	No	Number of SIP Subscribe attempts that failed due to policing on a trunk group.	
SIP_OTHER_REQ_FAIL_POLICING	COUNTER	No	Number of SIP other non-invite attempts that failed due to policing on trunk group.	
SIP_OTHER_REQ_FAIL_INTERNAL	COUNTER	No	The number of SIP other non-invite attempts that failed due to policing on a trunk group.	
SIP_OTHER_REQ_FAIL_OTHER	COUNTER	No	The number of SIP other non-invite attempts that failed due to policing on a trunk group.	
VIDEO_THRESH_HOLD_LIMIT	COUNTER	No	The number of video threshold limits that the specified interval for this trunk group exceeds.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

CallIntervalStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context

Column Name	Column Type	Index	Description	CLI Command Reference
ZNAME	STRING	Yes	The name of the address context zone.	
NAME	STRING	Yes	The name of this trunk group.	
IN_USAGE	COUNTER	No	The duration, in seconds, for which all inbound calls in a given interval are using the trunkgroup. This metric is derived using the formula: (total # of inbound calls on the TG) * (interval size) * 60	
OUT_USAGE	COUNTER	No	The duration, in seconds, for which all outbound calls in a given interval are using the trunkgroup. This metric is derived using the formula: (total # of outbound calls on the TG) * (interval size) * 60.	
IN_CALLS	COUNTER	No	Number of completed inbound calls on this trunk group for the specified interval.	
OUT_CALLS	COUNTER	No	Number of completed outbound calls on this trunk group for the specified interval.	
IN_CALL_ATTEMPTS	COUNTER	No	Number of inbound call attempts on this trunk group for the specified interval.	
OUT_CALL_ATTEMPTS	COUNTER	No	Number of outbound call attempts on this trunk group for the specified interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
MAX_COMPLETED_CALLS	COUNTER	No	The high watermark of total number of active calls in both the inbound and outbound directions on the trunk group for the specified interval. This statistic accounts for calls that are setting up, stable, or tearing down.	
CALL_SETUP_TIME	COUNTER	No	Total call setup time for all completed calls in inbound and outbound directions for this trunk group for specified interval measured in hundredths of a second.	
CALL_SETUPS	COUNTER	No	Total number of calls setup but not necessarily completed in the inbound and outbound directions for this trunk group for the specified interval.	
ROUTING_ATTEMPTS	COUNTER	No	The number of routing attempts for this trunk group for the specified interval. Each PSX dip can return up to 200 routes. The SBC selects routes based on a number of criteria such as CAC and bandwidth availability. In some cases, crankback/route advance is needed if the first selected route fails. This metric counts the number of routes attempted before the call succeeded. If the first route succeeds, this counter = 1.	

Column Name	Column Type	Index	Description	CLI Command Reference
IN_BW_USAGE	COUNTER	No	Sum of bandwidth usage (expected data rate in Kbits per second multiplied by call duration in seconds) for every inbound call associated with this trunk group for the specified interval.	
OUT_BW_USAGE	COUNTER	No	Sum of bandwidth usage (expected data rate in Kbits per second multiplied by call duration in seconds) in the outbound direction for this trunk group in seconds in the current interval. The trunk group usage is defined as the time a trunk is seized to the time a trunk is released.	
MAX_ACTIVE_BW_USAGE	GAUGE	No	High watermark bandwidth usage (in Kbits per second) in either direction associated with this trunk group for the specified interval.	
CALLS_WITH_PKT_OUTAGE	COUNTER	No	Number of calls with a maximum packet outage whose duration exceeds the configured minimum for this trunk group for the specified interval.	
CALLS_WITH_PKT_OUTAGE_AT_END	COUNTER	No	Number of calls whose maximum packet outage occurs at the end of the call for this trunk group for the specified interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
TOTAL_PKT_OUTAGE	COUNTER	No	Summation of packet outage durations (in milliseconds) whose duration exceeds the configured minimum which is reported during the specified performance interval.	
MAX_PKT_OUTAGE	GAUGE	No	Single longest maximum reported packet outage duration (in milliseconds) experienced during the specified performance interval for this trunk group.	
POD_EVENTS	COUNTER	No	Number of Packet Outage Detection (POD) Events detected for this peer group for the specified interval.	
PLAYOUT_BUFFER_GOOD	COUNTER	No	Number of calls with all sub-intervals reporting GOOD playout buffer quality for this trunk group for the specified interval.	
PLAYOUT_BUFFER_ACCEPTABLE	COUNTER	No	Number of calls with all sub-intervals reporting ACCEPTABLE or better playout buffer quality for this trunk group for the specified interval.	
PLAYOUT_BUFFER_POOR	COUNTER	No	Number of calls with all sub-intervals reporting POOR or better playout buffer quality for this trunk group for the specified interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
PLAYOUT_BUFFER_UNACCEPTABLE	COUNTER	No	Number of calls with at least one sub-interval reporting UNACCEPTABLE playout buffer quality for this trunk group for the specified interval.	
SIP_REG_ATTEMPTS	COUNTER	No	Current number of SIP registration attempts on a trunk group for the specified interval.	
SIP_REG_COMPLETIONS	COUNTER	No	Current number of SIP registrations that have successfully completed on a trunk group for the specified interval.	
CALLS_WITH_PBX_DIPS	COUNTER	No	The number of calls that made a PBX Dip during the interval (applies to ERE, ePBX and external ePBX).	

Column Name	Column Type	Index	Description	CLI Command Reference
TOTAL_PSX_DIPS	COUNTER	No	The total number of PSX dips for the specified interval (applies to ERE, ePSX and external ePSX). To see the number of calls which made PSX Dips during the interval, see <code>CALLS_WITH_PSX_DIPS</code> metric. Example During the specified interval, two calls made three dips each (due to call redirection, etc.) to the PSX. This is logged as: <pre>CALLS_WITH_P SX_DIPS = 2 and TOTAL_PSX_DIPS = 6.</pre> If calls do not involve redirection or other complex scenarios such as two-stage dialing and transfers, these two metrics can use the same value.	
ACTIVE_REGS	COUNTER	No	Interval number of active registrations on this trunk group.	
MAX_ACTIVE_REGS	GAUGE	No	Maximum active registrations on this trunk group (high-watermark achieved on this trunk group).	

Column Name	Column Type	Index	Description	CLI Command Reference
CALL_LIMIT	GAUGE	No	CALL_LIMIT is the summation of TOTAL_CALLS_AVAILABLE, INBOUND_CALLS_USAGE, PRIORITY_CALL_USAGE, and OUTBOUND_CALLS_USAGE from NBS5200TrunkGroupStatusStats table (when it is not unlimited). CALL_LIMIT is different from the Call Limit configured at the SBC 7000 device.	
ACTIVE_SUBS	COUNTER	No	Current number of active subscriptions on this trunk group.	
MAX_ACTIVE_SUBS	GAUGE	No	Maximum active subscriptions on this trunk group (high-watermark achieved on this trunk group).	
PEAK_CALL_RATE	GAUGE	No	The current system peak call arrival rate.	
ONGOING_CALLS	INTEGER	False	Total On Going Calls (Non-Stable + Stable) on this trunk group.	
STABLE_CALLS	INTEGER	False	Total Stable Calls on this trunk group.	
CALL_UPDATES	INTEGER	False	Total Call Updates on this trunk group.	

Column Name	Column Type	Index	Description	CLI Command Reference
EMERGENCY_STABLE_CALLS	INTEGER	False	Total Emergency Stable Calls on this trunk group.	
EMERGENCY_ONGOING_CALLS	INTEGER	False	Total Emergency Calls Stable + Non-Stable on this trunk group.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

NBS5200CallCountStats

Column Name	Column Type	Index	Description	CLI Command Reference
KEY	IMPLIEDSTRING	False	Key value for the call.	Show Table System
CALL_ATTEMPTS	COUNTER	True	Number of call attempts on this server.	
CALL_COMPLETIONS	COUNTER	True	Total number of completed call attempts on this server.	
ACTIVE_CALLS	GAUGE	True	Current number of active managed calls on this server.	
STABLE_CALLS	GAUGE	True	Current number of stable managed calls on this server.	
MAX_LICENSE_LIMIT	INTEGER	True	This object indicates maximum license limit of this server.	
CE_NAME	STRING	True	The name of the compute element for this entity.	

DiamNodeRfIntervalStatistics

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
DNAME	STRING	Yes	The name of this Diameter Node.	
NAME	STRING	Yes	The name of the peer.	
RF_SUCCESS	GAUGE	No	The count of successful ACR/ACA exchanged.	
RF_FAILED	GAUGE	No	The count of un-successful ACR/ACA exchanged.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

DnsGroupDnsServerStats

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	DNS Group - CLI
GNAME	STRING	Yes	The name of the address context group.	False	
IND	GAUGE	Yes	The DNS server statistics index for this address context.	False	
IP_ADDRESS	INETADDRESSES	No	The IP address of the DNS server requested for the statistics data.	False	
QUERIES	GAUGE	No	The number of queries made by the DNS client to this DNS server.	False	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
TIMEOUTS	GAUGE	No	The number of timeouts resulted from queries made by the DNSC client to this DNS server.	False	
ERRORS	GAUGE	No	The number of errors resulted from queries made by the DNSC client to this DNS server.	False	
REFERRALS	GAUGE	No	The number of referrals resulted from queries made by the DNSC client to this DNS server.	False	
TOTAL_TCP_CONNECTION	GAUGE	No	The number of tries for connecting to DNS server.	True	
TCP_CONNECTION_FAILED	GAUGE	No	The number of times SBC failed to connect to DNS server.	True	
TCP_CONNECTION_SUCCESS	GAUGE	No	The number of successful TCP connection to DNS server.	True	
TCP_CONNECTION_TORN_DOWN	GAUGE	No	The number of TCP connection torn down with DNS server.	True	
TCP_FALLBACK	GAUGE	No	The number of times tcp fallback with DNS server.	True	
EDNS_STATUSES	INTEGER	False	The number of times tcp fallback with DNS server.	True	
EDNS_FAILURES	GAUGE	False	The number of times tcp fallback with DNS server.	True	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

DSP Stats

DspResDspCallIntervalStats

Column Name	Column Type	Index	Description	CLI Command Reference
SYSTEM_NAME	STRING	Yes	Name of the system.	Show Table System
NUM_CALL_NO_DSP_ALLOC_FAIL	COUNTER	No	Number of call was successful without DSP resource allocation failure during an interval.	
NUM_CALL_WITH_DSP_ALLOC_FAIL	COUNTER	No	Number of call was successful with DSP resource allocation failure during an interval.	
NUM_CALL_FAIL_NO_G729	COUNTER	No	Number of call failed due to lack of G729 DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_G729	COUNTER	No	Number of call fails due to reason other than lack G729 DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_G729	COUNTER	No	Number of call was successful even though lack of G729 DSP resource during an interval.	
NUM_CALL_FAIL_NO_G726	COUNTER	No	Number of call failed due to lack of G726 DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_OTHER_ON_G726	COUNTER	No	Number of call fails due to reason other than lack G726 DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_G726	COUNTER	No	Number of call was successful even though lack of G726 DSP resource during an interval.	
NUM_CALL_FAIL_NO_G711_PACKET	COUNTER	No	Number of call failed due to lack of G711 Packet DSP resource during an interval.	
NUM_CALL_FAIL_ON_G711_PACKET	COUNTER	No	Number of call fails due to reason other than lack G711 Packet DSP resource during an interval.	
NUM_CALL_NO_G711_PACKET	COUNTER	No	Number of call was successful even though lack of G711 Packet DSP resource during an interval.	
NUM_CALL_FAIL_NO_G723	COUNTER	No	Number of call failed due to lack of G723 DSP resource during an interval.	
NUM_CALL_FAIL_ON_G723	COUNTER	No	Number of call fails due to reason other than lack G723 DSP resource during an interval.	
NUM_CALL_NO_G723	COUNTER	No	Number of call was successful even though lack of G723 DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_NO_ILBC	COUNTER	No	Number of call failed due to lack of ILBC DSP resource during an interval.	
NUM_CALL_FAIL_ON_ILBC	COUNTER	No	Number of call fails due to reason other than lack ILBC DSP resource during an interval.	
NUM_CALL_NO_ILBC	COUNTER	No	Number of call was successful even though lack of ILBC DSP resource during an interval.	
NUM_CALL_FAIL_NO_EVRCB	COUNTER	No	Number of call failed due to lack of EVRCB0 DSP resource during an interval.	
NUM_CALL_FAIL_ON_EVRCB	COUNTER	No	Number of call fails due to reason other than lack EVRCB0 DSP resource during an interval.	
NUM_CALL_NO_EVRCB	COUNTER	No	Number of call was successful even though lack of EVRCB0 DSP resource during an interval.	
NUM_CALL_FAIL_NO_GSM	COUNTER	No	Number of call failed due to lack of AMRNB DSP resource during an interval.	
NUM_CALL_FAIL_ON_GSM	COUNTER	No	Number of call fails due to reason other than lack AMRNB DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_NO_GSM	COUNTER	No	Number of call was successful even though lack of AMRNB DSP resource during an interval.	
NUM_CALL_FAIL_NO_AMRWB	COUNTER	No	Number of call failed due to lack of AMRWB DSP resource during an interval.	
NUM_CALL_FAIL_ON_AMRWB	COUNTER	No	Number of call fails due to reason other than lack AMRWB DSP resource during an interval.	
NUM_CALL_NO_AMRWB	COUNTER	No	Number of call was successful even though lack of AMRWB DSP resource during an interval.	
NUM_CALL_FAIL_NO_G722	COUNTER	No	Number of call failed due to lack of G722 DSP resource during an interval.	
NUM_CALL_FAIL_ON_G722	COUNTER	No	Number of call fails due to reason other than lack G722 DSP resource during an interval.	
NUM_CALL_NO_G722	COUNTER	No	Number of call was successful even though lack of G722 DSP resource during an interval.	
NUM_CALL_FAIL_NO_TONE	COUNTER	No	Number of call failed due to lack of TONE DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_ON_TONE	COUNTER	No	Number of call fails due to reason other than lack TONE DSP resource during an interval.	
NUM_CALL_NO_TONE	COUNTER	No	Number of call was successful even though lack of TONE DSP resource during an interval.	
NUM_CALL_FAIL_NO_EVRC	COUNTER	No	Number of call failed due to lack of EVRC DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_EVRC	COUNTER	No	Number of call fails due to reason other than lack EVRC DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_EVRC	COUNTER	No	Number of call was successful even though lack of EVRC DSP resource during an interval.	
NUM_CALL_FAIL_NO_G7221	COUNTER	No	Number of call failed due to lack of G7221 DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_G7221	COUNTER	No	Number of call fails due to reason other than lack G7221 DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_G7221	COUNTER	No	Number of call was successful even though lack of G7221 DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_NO_EFR	COUNTER	No	Number of call failed due to lack of Efr DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_EFR	COUNTER	No	Number of call fails due to reason other than lack Efr DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_EFR	COUNTER	No	Number of call was successful even though lack of Efr DSP resource during an interval.	
NUM_CALL_FAIL_NO_OPUS	COUNTER	No	Number of call failed due to lack of OPUS DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_OPUS	COUNTER	No	Number of call fails due to reason other than lack of OPUS DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_OPUS	COUNTER	No	Number of call was successful even though lack of OPUS DSP resource during an interval.	
NUM_CALL_FAIL_NO_SILK8	COUNT	No	Number of calls failed due to lack of SILK_8 DSP resource	
NUM_CALL_FAIL_OTHER_SILK8	COUNT	No	Number of calls failed due to reason other than lack of SILK_8 DSP resource	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_SUCCESS_NO_SILK8	COUNT	No	Number of calls successful even with lack of SILK_8 DSP resource	
NUM_CALL_FAIL_NO_SILK16	COUNT	No	Number of calls successful even with lack of SILK_8 DSP resource	
NUM_CALL_FAIL_OTHER_SILK16	COUNT	No	Number of calls failed due to reason other than lack of SILK_16 DSP resource	
NUM_CALL_SUCCESS_NO_SILK16	COUNT	No	Number of calls successful even with lack of SILK_16 DSP resource	
NUM_CALL_FAIL_NO_EVS	INTEGER	No	The number of call fails due to the lack of EVS DSP resource during a time interval.	
NUM_CALL_FAIL_OTHER_EVS	INTEGER	No	The number of call fails due to a reason other than the lack of EVS DSP resource during a time interval.	
NUM_CALL_SUCCESS_NO_EVS	INTEGER	No	The number of calls was successful despite the lack of EVS DSP resource during a time interval.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

DspResDspUsageIntervalStats

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
SYSTEM_NAME	STRING	Yes	Name of the system.		Show Table System
G729_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G729 DSP pad during an interval time.		
G729_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G729 DSP pad during an interval time.		
G729_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G729 DSP pad during an interval time.		
G726_PEAK_USED_COUNT	GAUGE	No	The Interval number of Peak usage of type G726 DSP pad during an interval time.		
G726_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G726 DSP pad during an interval time.		
G726_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G726 DSP pad during an interval time.		
G711_PACKET_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711Packet DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711_PACKET_AVG_USED_COUNT	GAUGE	No	The average usage of type G711Packet DSP pad during an interval time.		
G711_PACKET_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711Packet DSP pad during an interval time.		
G723_PEAK_USED_COUNT	GAUGE	No	The Interval number of Peak usage of type G723 DSP pad during an interval time.		
G723_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G723 DSP pad during an interval time.		
G723_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G723 DSP pad during an interval time.		
ILBC_PEAK_USED_COUNT	GAUGE	No	The peak usage of type ILBC DSP pad during an interval time.		
ILBC_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type ILBC DSP pad during an interval time.		
ILBC_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type ILBC DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
EVRCB0_PEAK_USED_COUNT	GAUGE	No	The peak usage of type EVRCB0 DSP pad during an interval time.		
EVRCB0_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type EVRCB0 DSP pad during an interval time.		
EVRCB0_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type EVRCB0 DSP pad during an interval time.		
GSM_PEAK_USED_COUNT	GAUGE	No	The peak usage of type AMRNB DSP pad during an interval time.		
GSM_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type AMRNB DSP pad during an interval time.		
GSM_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type AMRNB DSP pad during an interval time.		
AMRWB_PEAK_USED_COUNT	GAUGE	No	The peak usage of type Amrwb DSP pad during an interval time.		
AMRWB_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type Amrwb DSP pad during an interval time.		
AMRWB_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type Amrwb DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G722_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 DSP pad during an interval time.		
G722_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G722 DSP pad during an interval time.		
G722_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G722 DSP pad during an interval time.		
TONE_PEAK_USED_COUNT	GAUGE	No	The peak usage of type TONE DSP pad during an interval time.		
TONE_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type TONE DSP pad during an interval time.		
TONE_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type TONE DSP pad during an interval time.		
EVRC_PEAK_USED_COUNT	GAUGE	No	The peak usage of type EVRCB0 DSP pad during an interval time.		
EVRC_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type EVRC DSP pad during an interval time.		
EVRC_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type EVRC DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G7221_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G7221 DSP pad during an interval time.		
G7221_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G7221 DSP pad during an interval time.		
G7221_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G7221 DSP pad during an interval time.		
EFR_PEAK_USED_COUNT	GAUGE	No	The peak usage of type Efr DSP pad during an interval time.		
EFR_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type Efr DSP pad during an interval time.		
EFR_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type Efr DSP pad during an interval time.		
G711SS_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711Ss DSP pad during an interval time.		
G711SS_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G711Ss DSP pad during an interval time.		
G711SS_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G711Ss DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G729V8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G729 V8 DSP pad during an interval time.		
G729V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G729 V8 DSP pad during an interval time.		
G729V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G729 V8 DSP pad during an interval time.		
G726V8_PEAK_USED_COUNT	GAUGE	No	The Interval number of Peak usage of type G726 V8 DSP pad during an interval time.		
G726V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G726 V8 DSP pad during an interval time.		
G726V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G726 V8 DSP pad during an interval time.		
G711V8_PACKET_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711Packet V8 DSP pad during an interval time.		
G711V8_PACKET_AVG_USED_COUNT	GAUGE	No	The average usage of type G711Packet V8 DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711V8_PACKET_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711Packet V8 DSP pad during an interval time.		
G711SSV8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711SSPacket V8 DSP pad during an interval time.		
G711SSV8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G711SSPacket V8 DSP pad during an interval time.		
G711SSV8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G711SSPacket V8 DSP pad during an interval time.		
G723V8_PEAK_USED_COUNT	GAUGE	No	The Interval number of Peak usage of type G723 V8 DSP pad during an interval time.		
G723V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G723 V8 DSP pad during an interval time.		
G723V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G723 V8 DSP pad during an interval time.		
ILBCV8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type ILBC V8 DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
ILBCV8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type ILBC V8 DSP pad during an interval time.		
ILBCV8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type ILBC V8 DSP pad during an interval time.		
G722V8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 V8 DSP pad during an interval time.		
G722V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G722 V8 DSP pad during an interval time.		
G722V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G722 V8 DSP pad during an interval time.		
G7221V8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722.1 V8 DSP pad during an interval time.		
G7221V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G722.1 V8 DSP pad during an interval time.		
G7221V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G722.1 V8 DSP pad during an interval time.		
OPUS_PEAK_USED_COUNT	GAUGE	No	The peak usage of type OPUS DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
OPUS_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type OPUS DSP pad during an interval time.		
OPUS_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type OPUS DSP pad during an interval time.		
EVS_PEAK_USED_COUNT	GAUGE	No	The peak usage of type EVS DSP pad during an interval time.		
EVS_AVG_USED_COUNT	GAUGE	No	The average usage of type EVS DSP pad during an interval time.		
EVS_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type EVS DSP pad during an interval time.		
SILK8_PEAK_USED_COUNT	COUNT	No	Peak usage of type SILK_8 DSP PAD		
SILK8_AVG_USED_COUNT	COUNT	No	Average usage of type SILK_8 DSP PAD		
SILK8_AVG_AVAIL_COUNT	COUNT	No	Average availability of type SILK_8 DSP PAD		
SILK16_PEAK_USED_COUNT	COUNT	No	Peak usage of type SILK_16 DSP PAD		
SILK16_AVG_USED_COUNT	COUNT	No	Average usage of type SILK_16 DSP PAD		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
SILK16_AVG_AVAIL_COUNT	COUNT	No	Average availability of type SILK_16 DSP PAD		
AMRWT140_PEAK_USED_COUNT	INTEGER	No	The peak usage of AMR with T.140 DSP pad in a predefined interval.		
AMRWT140_AVG_USED_COUNT	INTEGER	No	The average usage of AMR with T.140 DSP pad in a predefined interval.		
AMRWT140_AVG_AVAIL_COUNT	INTEGER	No	The average availability of AMR with T.140 DSP pad in a predefined interval.		
AMRWBT140_PEAK_USED_COUNT	INTEGER	No	The peak usage of AMRWB with T.140 DSP pad in a predefined interval.		
AMRWT140_AVG_USED_COUNT	INTEGER	No	The average usage of AMR with T.140 DSP pad in a predefined interval.		
AMRWT140_AVG_AVAIL_COUNT	INTEGER	No	The average availability of AMR with T.140 DSP pad in a predefined interval.		
AMR_PEAK_USAGE_COUNT	GAUGE	No	The current peak usage of type AMRNB DSP PAD.		
AMR_AVG_USAGE_COUNT	GAUGE	No	The current average usage of type AMRNB DSP PAD.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
AMR_AVG_A VAIL_COUNT	GAUGE	No	The current average availability of type AMRNB DSP PAD.		
EVS_T140_P EAK_USED_ COUNT	GAUGE	No	The peak usage of type EVS with T.140 DSP pad during an interval time.		
EVS_T140_A VERAGE_US ED_COUNT	GAUGE	No	The average usage of type EVS with T.140 DSP pad during an interval time.		
EVS_T140_A VERAGE_AVA IL_COUNT	GAUGE	No	The average availability of type EVS with T.140 DSP pad during an interval time.		
G711T140_PE AK_USED_C OUNT	GAUGE	No	The average availability of type EVS with T.140 DSP pad during an interval time.	MEAN	
G711T140_AV G_USED_CO UNT	GAUGE	No	The average usage of type G711 with T.140 DSP pad during an interval time.	MEAN	
G711T140_AV G_AVAIL_CO UNT	GAUGE	No	The average availability of type G711 with T.140 DSP pad during an interval time.	MEAN	
G711SST140_ PEAK_USED_ COUNT	GAUGE	No	The peak usage of type G711SS with T.140 DSP pad during an interval time.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SST140_AVG_USED_COUNT	GAUGE	No	The average usage of type G711SS with T.140 DSP pad during an interval time.	MEAN	
G711SST140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711SS with T.140 DSP pad during an interval time.	MEAN	
OPUST140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type Opus with T.140 DSP pad during an interval time.	MEAN	
OPUST140_AVG_USED_COUNT	GAUGE	No	The average usage of type Opus with T.140 DSP pad during an interval time.	MEAN	
OPUST140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type Opus with T.140 DSP pad during an interval time.	MEAN	
G722T140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 with T.140 DSP pad during an interval time.	MEAN	
G722T140_AVG_USED_COUNT	GAUGE	No	The average usage of type G722 with T.140 DSP pad during an interval time.	MEAN	
G722T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G722 with T.140 DSP pad during an interval time.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G722V8T140_ PEAK_USED_ COUNT	GAUGE	No	The peak usage of type G722 V8 with T.140 DSP pad during an interval time.	MEAN	
G722V8T140_ AVG_USED_ COUNT	GAUGE	No	The average usage of type G722 V8 with T.140 DSP pad during an interval time.	MEAN	
G722V8T140_ AVG_AVAIL_C OUNT	GAUGE	No	The average availability of type G722 V8 with T.140 DSP pad during an interval time.	MEAN	
G711T140V8_ PEAK_USED_ COUNT	GAUGE	No	The peak usage of type G711 V8 with T.140 DSP pad during an interval time.	MEAN	
G711T140V8_ AVG_USED_ COUNT	GAUGE	No	The average usage of type G711 V8 with T.140 DSP pad during an interval time.	MEAN	
G711T140V8_ AVG_AVAIL_C OUNT	GAUGE	No	The average availability of type G711 V8 with T.140 DSP pad during an interval time.	MEAN	
G711SSV8T1 40_PEAK_US ED_COUNT	GAUGE	No	The peak usage of type G711SS V8 with T.140 DSP pad during an interval time.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SSV8T140_AVG_USAGE_COUNT	GAUGE	No	The average usage of type G711SS V8 with T.140 DSP pad during an interval time.	MEAN	
G711SSV8T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711SS V8 with T.140 DSP pad during an interval time.	MEAN	
L16_PEAK_USAGE_COUNT	GAUGE	No	The peak usage of type L16 DSP pad during an interval time.	MEAN	
L16_AVG_USAGE_COUNT	GAUGE	No	The average usage of type L16 DSP pad during an interval time.	MEAN	
L16_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type L16 DSP pad during an interval time.	MEAN	
CE_NAME	STRING	No	The name of the compute element for this entity.	N/A	

EthernetPortMgmtStats

Column Name	Column Type	Index	Description	CLI Command Reference
PORT_NAME	STRING	Yes	The name of this port.	Ethernet Port - CLI
RX_PACKETS	COUNTER64	No	The number of received packets.	
TX_PACKETS	COUNTER64	No	The number of transmitted packets.	

Column Name	Column Type	Index	Description	CLI Command Reference
RX_ERRORS	COUNTER	No	The number of bad packets received	
TX_ERRORS	COUNTER	No	The number of packet transmit failures.	
RX_DROPPED	COUNTER	No	The number of packets dropped due to no receive buffers.	
TX_DROPPED	COUNTER	No	The number of packets dropped due to no transmit buffers.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

EthernetPortPacketStats

Column Name	Column Type	Index	Description	CLI Command Reference
PORT_NAME	STRING	Yes	The name of this port.	Ethernet Port - CLI
RX_PACKETS	COUNTER64	No	The number of received packets.	
TX_PACKETS	COUNTER64	No	The number of transmitted packets.	
RX_ERRORS	COUNTER	No	The number of bad packets received.	
TX_ERRORS	COUNTER	No	The number of packet transmit failures.	
RX_DROPPED	COUNTER	No	The number of packets dropped due to no receive buffers.	
TX_DROPPED	COUNTER	No	The number of packets dropped due to no transmit buffers.	

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	No	The name of the compute element for this entity.	

H323SigPortStatisticsStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context zone.	
NAME	STRING	Yes	The name of this H323 Signaling Port.	
IND	GAUGE	Yes	The index of this H323 Signaling Port.	
STATUS	INTEGER	No	Status of the H323 Signaling Port.	
INGRESS_CALLS_COMPLETED	INTEGER	No	Number of Ingress calls completed since system boot up.	
EGRESS_CALLS_COMPLETED	INTEGER	No	Number of Egress calls completed since system boot up.	
INGRESS_CALLS_ATTEMPTED	INTEGER	No	Number of Ingress calls attempted since system boot up.	
EGRESS_CALLS_ATTEMPTED	INTEGER	No	Number of Egress calls attempted since system boot up.	
H225_MESSAGES_SENT	COUNTER64	No	Number of H225 messages that sent since system boot up.	

Column Name	Column Type	Index	Description	CLI Command Reference
H225_MESSAGE_BYTES_SENT	COUNTER64	No	Number of bytes of H225 messages that sent since system boot up.	
H225_MESSAGES_RCVD	COUNTER64	No	Number of H225 messages that are received since system boot up.	
H225_MESSAGE_BYTES_RCVD	COUNTER64	No	Number of bytes of H225 messages that are received since system boot up.	
H245_MESSAGES_SENT	COUNTER64	No	Number of H245 messages that sent since system boot up.	
H245_MESSAGE_BYTES_SENT	COUNTER64	No	Number of bytes of H245 messages that sent since system boot up.	
H245_MESSAGES_RCVD	COUNTER64	No	Number of H245 messages that are received since system boot up.	
H245_MESSAGE_BYTES_RCVD	COUNTER64	No	Number of bytes of H245 messages that are received since system boot up.	
ACTIVE_CALLS	INTEGER	No	Number of Active calls at this moment.	
H225_TCP_PORTS_OPENED	INTEGER	No	Number of H225 TCP ports opened at this moment.	
H245_TCP_PORTS_OPENED	INTEGER	No	Number of H245 TCP ports opened at this moment.	
H245_TCP_PORTS_ALLOCATED	INTEGER	No	Number of H245 TCP ports allocated at this moment.	

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	No	The name of the compute element for this entity.	

IcmpGeneralGroupStats

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	The name of the compute element for this entry.	NA
IN_MSGS	COUNTER	No	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.	
IN_ECHOS	COUNTER	No	The number of ICMP Echo (request) messages received.	
IN_ECHO_REPS	COUNTER	No	The number of ICMP Echo Reply messages received.	
IN_DEST_UNREACHS	COUNTER	No	The number of ICMP Destination Unreachable messages received.	
IN_ERRORS	COUNTER	No	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).	
OUT_MSGS	COUNTER	No	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.	

Column Name	Column Type	Index	Description	CLI Command Reference
OUT_ERRORS	COUNTER	No	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations, any type of error that contributes to the value of this counter may not exist.	
OUT_ECHOS	COUNTER	No	The number of ICMP Echo (request) messages sent.	
OUT_ECHO_REPS	COUNTER	No	The number of ICMP Echo Reply messages sent.	
OUT_DEST_UNREACHS	COUNTER	No	The number of ICMP Destination Unreachable messages sent.	

IP Stats

IpAclOverallStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	IP Access Control List - Non-Cloud - CLI
NAME	IMPLIEDSTRING	Yes	The name of the address context.	
MATCHED_NO_RULE	COUNTER	No	The number of times no rule is matched.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

IpAclRuleStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	IP Access Control List - Non-Cloud - CLI
NAME	STRING	Yes	The name of this IP access control list rule.	
MATCHES	COUNTER	No	The number of times this rule is matched.	
POLICER_DISCARDS	COUNTER	No	The number of times the policer for this rule discarded packets.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

IpGeneralGroupStats

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	The name of the compute element for this entry.	NA
IN_RECEIVES	COUNTER	No	The total number of input datagrams received from interfaces, including those received in error.	
IN_HDR_ERRORS	COUNTER	No	The number of input datagrams discarded due to errors such as errors in IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options.	

Column Name	Column Type	Index	Description	CLI Command Reference
IN_ADDR_ERR ORS	COUNTER	No	The number of input datagrams discarded because the IP address in the destination field of the IP header was not a valid address this entity could receive. This count includes invalid addresses (for example, 0.0.0.0) and addresses of unsupported Classes (for example, Class E). For entities which are not IP routers and do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.	
IN_UNKNOWN_ PROTOS	COUNTER	No	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.	
IN_DISCARDS	COUNTER	No	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.	
IN_DELIVERS	COUNTER	No	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).	

Column Name	Column Type	Index	Description	CLI Command Reference
OUT_REQUESTS	COUNTER	No	The total number of IP datagrams which local IP user- protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.	
OUT_DISCARDS	COUNTER	No	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). Note that this counter includes datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.	
OUT_NO_ROUTEES	COUNTER	No	The number of IP datagrams discarded because no route can transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this no-route criterion. This also includes any datagrams which a host cannot route because all of its default routers are down.	
REASM_TIMEOUT	INTEGER	No	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.	
REASM_REQDS	COUNTER	No	The number of IP fragments received that this entity must reassemble.	
REASM_OKS	COUNTER	No	The number of IP datagrams successfully re-assembled.	

Column Name	Column Type	Index	Description	CLI Command Reference
REASM_FAILS	COUNTER	No	The number of failures detected by the IP re-assembly algorithm (for reasons such as timed out, errors). Note that this is not necessarily a count of discarded IP fragments since some algorithms (like the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.	
FRAG_OKS	COUNTER	No	The number of IP datagrams successfully fragmented at this entity.	
FRAG_FAILS	COUNTER	No	The number of IP datagrams discarded because this entity must, but cannot, fragment them. For example, because their Don't Fragment flag was set.	

IpPolicingSystemIntStats

Column Name	Column Type	Index	Description	CLI Command Reference
SYSTEM_NAME	STRING	Yes	Name of the system.	IP Policing - CLI
BAD_HDR_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the bad Ethernet/IP Header policer.	
BAD_HDR_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the bad Ethernet/IP Header policer.	
BAD_HDR_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the bad Ethernet/IP Header policer.	

Column Name	Column Type	Index	Description	CLI Command Reference
BAD_HDR_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the bad Ethernet/IP Header policer.	
BAD_HDR_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the bad Ethernet/IP Header policer.	
BAD_HDR_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the bad Ethernet/IP Header policer.	
ARP_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the ARP policer.	
ARP_ACCEPT_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the ARP policer.	
ARP_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the ARP policer.	
ARP_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the ARP policer.	
ARP_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the ARP policer.	
ARP_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the ARP policer.	
ARP_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the ARP policer.	

Column Name	Column Type	Index	Description	CLI Command Reference
UFLOW_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the micro flow policer.	
UFLOW_ACCEPT_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the micro flow policer.	
UFLOW_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the micro flow policer.	
UFLOW_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the micro flow policer.	
UFLOW_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the micro flow policer.	
UFLOW_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the micro flow policer.	
UFLOW_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the micro flow policer.	
ACL_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the access control list policer.	
ACL_ACCEPT_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the access control list policer.	
ACL_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the access control list policer.	

Column Name	Column Type	Index	Description	CLI Command Reference
ACL_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the access control list policer.	
ACL_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the access control list policer.	
ACL_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the access control list policer.	
ACL_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the access control list policer.	
AGGREGATE_DISCARD_PKT_COUNT	COUNTER64	No	The current number of discarded packets for the aggregate policer.	
AGGREGATE_ACCEPT_PKT_COUNT	COUNTER64	No	The current number of discarded packets for the aggregate policer.	
AGGREGATE_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the aggregate policer.	
AGGREGATE_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the aggregate policer.	
AGGREGATE_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the aggregate policer.	
AGGREGATE_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the aggregate policer.	

Column Name	Column Type	Index	Description	CLI Command Reference
AGGREGATE_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the aggregate policer.	
IP_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the IPSEC Decrypt policer.	
IP_ACCEPT_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the IPSEC Decrypt policer.	
IP_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the IPSEC Decrypt policer.	
IP_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the IPSEC Decrypt policer.	
IP_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the IPSEC Decrypt policer.	
IP_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the IPSEC Decrypt policer.	
IP_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the IPSEC Decrypt policer.	
MEDIA_DISCARD_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the media policer.	
MEDIA_ACCEPT_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the media policer.	

Column Name	Column Type	Index	Description	CLI Command Reference
MEDIA_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the media policer.	
MEDIA_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the media policer.	
MEDIA_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the media policer.	
MEDIA_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the media policer.	
MEDIA_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the media policer.	
ROGUE_MEDIA_DISCARD_PKT_COUNT	COUNTER64	No	The current number of discarded packets for the rogue media policer.	
ROGUE_MEDIA_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the rogue media policer.	
ROGUE_MEDIA_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the rogue media policer.	
ROGUE_MEDIA_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the rogue media policer.	
ROGUE_MEDIA_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the rogue media policer.	

Column Name	Column Type	Index	Description	CLI Command Reference
ROGUE_MEDIA_MAJOR_ALARM_DUR	COUNTER	No	The current duration of the major alarms in seconds for the rogue media policer.	
DISCARD_RULE_PACKET_COUNT	COUNTER64	No	The current number of discarded packets for the IPSEC Decrypt policer.	
DISCARD_PEAK_DISCARD_RATE	GAUGE	No	The current peak discard rate for the discard rule.	
DISCARD_MINOR_ALARM_COUNT	COUNTER	No	The current number of minor alarms for the discard rule.	
DISCARD_MINOR_ALARM_DURATION	COUNTER	No	The current duration of the minor alarms in seconds for the discard rule.	
DISCARD_MAJOR_ALARM_COUNT	COUNTER	No	The current number of major alarms for the discard rule.	
DISCARD_MAJOR_ALARM_DURATION	COUNTER	No	The current duration of the major alarms in seconds for the discard rule.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

Link Stats

LinkDetectionGroupStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Link Detection Group - CLI

Column Name	Column Type	Index	Description	CLI Command Reference
NAME	STRING	Yes	The link failure statistics per trunk group.	
SINGLE_FAILURES	INTEGER	No	The number of times a link monitor within this link detection group failed to receive a single echo reply. The first reattempt was successful.	
DOUBLE_FAILURES	INTEGER	No	The number of times a link monitor within this link detection group failed to receive two consecutive echo replies. The second (next) reattempt was successful.	
FAILURES	INTEGER	No	The number of times a link monitor within this link detection group declared itself failed.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

LinkMonitorStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Link Detection Group - CLI
GNAME	STRING	Yes	The name of the address context group.	
NAME	STRING	Yes	The name of the link monitor that monitors a link to a destination for a specific interface.	
MIN_TIME	INTEGER	No	The minimum time (in microseconds) used to get a reply for an echo request packet.	

Column Name	Column Type	Index	Description	CLI Command Reference
MAX_TIME	INTEGER	No	The maximum time (in microseconds) used to get a reply for an echo request packet.	
AVERAGE_TIME	INTEGER	No	The average time (in microseconds) used to get a reply for an echo request packet.	
SINGLE_FAILURES	INTEGER	No	The number of single failures for this IP interface.	
DOUBLE_FAILURES	INTEGER	No	The number of double failures for this IP interface.	
FAILURES	INTEGER	No	The number of failures for this IP interface.	
REPLIES	INTEGER	No	The total number of replies.	
DUPLICATE_REPLIES	INTEGER	No	The number of duplicate replies.	
LATE_REPLIES	INTEGER	No	The number of late replies.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

SipLocalRegistrarRegCountIntStats

Column Name	Column Type	Description	Index	canAggregate
NAME	INTEGER	The name of the system.	True	False
SIP_REG_ATTEMPT_COUNT	GAUGE	The number of SIP registration attempts	False	True
SIP_REG_CHALLENGED_COUNT	GAUGE	The current number of challenged SIP registrations	False	True

Column Name	Column Type	Description	Index	canAggregate
SIP_REG_FAILED_403_COUNT	GAUGE	The total number of SIP registrations failed with 403	False	True
SIP_REG_FAILED_404_COUNT	GAUGE	The total number of SIP registrations failed with 404	False	True
SIP_REG_FAILED_503_COUNT	GAUGE	The total number of SIP registrations failed with 503	False	True
SIP_REG_FAILED_OTHERS_COUNT	GAUGE	The total number of SIP registrations failed with other response codes	False	True
SIP_REG_STABLE_COUNT	GAUGE	The current number of stable SIP registrations	False	True
LICENSE_MODE (Metric column)	INTEGER	It is copy of SBX7KLicenseUsageStats.LICENSE_MODE	False	True
CE_NAME	STRING	The name of the compute element for this entity.	False	False

NBS5200TrunkGroupStatusStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of this Address Context.	Show Table System
ZNAME	STRING	Yes	The name of this Zone.	
NAME	STRING	Yes	The name of this IP trunk group.	
STATE	INTEGER	No	Current operational state of the IP trunk group.	
TOTAL_CALLS_AVAILABLE	GAUGE	No	The sum of all available or unblocked calls for this trunk group.	

Column Name	Column Type	Index	Description	CLI Command Reference
TOTAL_CALLS_INBOUND_RESERVED	GAUGE	No	The reserved count as specified by the percentage configured for this IP trunk group. This object shows the total number of calls that are reserved for inbound calls on this IP trunk group. This is applicable only for IP trunk groups that are configured for inbound or both directions.	
INBOUND_CALLS_USAGE	GAUGE	No	The current inbound or incoming usage count of this IP trunk group. This is applicable only for IP trunk groups that are configured for inbound or both directions.	
OUTBOUND_CALLS_USAGE	GAUGE	No	The current outbound, non-priority usage count of this IP trunk group.	
TOTAL_CALLS_CONFIGURED	GAUGE	No	The total number of calls that are configured on this IP trunk group.	
PRIORITY_CALL_USAGE	GAUGE	No	The current priority usage count of this IP trunk group. This is applicable for IP trunk groups that are configured with call reserved state enabled.	
TOTAL_OUTBOUND_CALLS_RESERVED	GAUGE	No	The reserved count as specified by the percentage configured for this IP trunk group. This object reflects the total number of calls that are reserved for outbound calls on this IP trunk group. This is applicable for IP trunk groups that are configured for incoming call reservation.	

Column Name	Column Type	Index	Description	CLI Command Reference
BW_CURRENT_LIMIT	INTEGER	No	The current bandwidth limit for this IP trunk group. It is initially set to the configured bandwidth limit but the packet outage detection events may reduce the limit.	
BW_AVAILABLE	INTEGER	No	Bandwidth available for allocation.	
BW_INBOUND_USAGE	GAUGE	No	Bandwidth in use for inbound traffic.	
BW_OUTBOUND_USAGE	GAUGE	No	Bandwidth in use for outbound traffic.	
PACKET_OUT_DETECT_STATE	INTEGER	No	This object indicates the packet outage detection state. - normal - No packet outage is declared - packetOutageState - Packet outage is declared The packet outage detection bandwidth limit reduction reduces the current bandwidth limit.	
TG_UTIL_PERCENT	INTEGER	No	This is calculated as: $\left(\frac{((\text{PSTN\_INBOUND\_USAGE} + \text{PSTN\_OUTBOUND\_USAGE}) * 100)}{\text{PSTN\_TOTAL\_CONFIGURED}} \right)$	
PRIORITY_BW_USAGE	GAUGE	No	The current media bandwidth in use for oversubscribed HPC/emergency calls (in Kbits/sec).	
CE_NAME	STRING	No	The name of the compute element for this entity.	

RelayIntervalStatistics

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context
KEY	STRING	Yes	Key value for the call.	False	
NEW_CONN_CREATED	GAUGE	No	Total number of new relay connections created.	True	
CONN_TERM_GRACEFULLY	GAUGE	No	The number of connections terminated gracefully.	True	
CONN_TERM_NON_GRACEFULLY	GAUGE	No	The number of connections terminated non-gracefully.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SBCORE Stats

SBCCOREFacBlockingStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate type
KEY_TYPE	STRING	true	Key type such as call-id and calling party number.	False	N/A
KEY_ENTITY	STRING	true	Key values of call-id and calling party number.	False	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate type
BLOCK_CO UNT	INTEGER	false	The count of incoming packets dropped because of matching key/value pair of packet. The count is reset when a blocking entry is removed from the list. The entry is removed if the crash count is less than the configured threshold count or the entry is part of the facNonBlockingEntries list.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entity.	False	N/A

SBCCOREFacTotBlockStats

Column Name	Column Type	Index	Description	canAggregate
KEY_VAL	STRING	true	The dummy key for the list. At least one entry in the list is non-key.	False
TOTAL_BLOCK_CO UNT	INTEGER	false	The count of packets dropped due to all blocking entries.	True
CE_NAME	STRING	No	The name of the compute element for this entity.	False

SBCCOREOodMessageIntStats

Column Name	Column Type	Index	Description	canAggregate
MESSAGE_RATE	COUNT	False	Number of incoming OOD requests received per second.	False
CE_NAME	STRING	No	The name of the compute element for this entity.	False

SBCCORESipIPResIntStats

Column name	Column type	Index	Description	canAggregate
ACNAME	STRING	True	The name of this Address Context.	False

Column name	Column type	Index	Description	canAggregate
ZNAME	STRING	True	The name of this Zone.	False
NAME	STRING	True	The name of this SIP IP Peer.	False
DIRECTION	STRING	True	The direction of (Interval) SIP response messages.	False
RESCODE	INTEGER	True	The response code of (Interval) SIP response messages.	False
RESCOUNT	INTEGER	False	The total number of (Interval) SIP response messages for the specified response code.	True
CE_NAME	STRING	No	The name of the compute element for this entity.	False

SBCCORESipRegCountDomIntStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	true	The name of the address context.	False
DOMAIN_NAME	STRING	true	Domain name of the registration.	False
COUNT_ATTEMPTS	COUNTER	true	The number of SIP registration attempts.	False
COUNTCUM_COMPLETED	COUNTER	false	The accumulative number of completed SIP registration attempts.	True
COUNT_PENDING	COUNTER	false	The current number of pending SIP registrations.	True
COUNT_STABLE	COUNTER	false	The current number of stable SIP registrations.	True
COUNT_TOTAL	COUNTER	false	The total number of current SIP registrations.	True

Column Name	Column Type	Index	Description	canAggregate
EMERGENCY_ACC_TOT	COUNTER	false	The total number of accepted emergency SIP registrations.	True
EMERGENCY_COUNT_ACT	COUNTER	false	The total number of active emergency SIP registrations.	True
CE_NAME	STRING	No	The name of the compute element for this entity.	False

Note

SipSigConnStatisticsStats is not supported from SBC 4.1 onwards.

SBCCORESipTgCSSRIntStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	true	The name of the address context.	false
ZNAME	STRING	true	The name of the address context zone.	false
NAME	STRING	true	The name of this SIP trunk group.	false
INV_SENT	COUNTER	false	The total number of (interval) inv_sent.	true
INV_RCVD	COUNTER	false	The total number of (interval) inv_rcvd.	true
ALERT_SENT	COUNTER	false	The total number of (interval) 18x_sent.	true
ALERT_RCVD	COUNTER	false	The total number of (interval) 18x_rcvd.	true
ANSCALLS_SENT	COUNTER	false	The total number of (interval) ansCalls_sent.	true
ANSCALLS_RCVD	COUNTER	false	The total number of (interval) ansCalls_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
CANCEL_SENT	COUNTER	false	The total number of (interval) cancel_sent.	true
CANCEL_RCVD	COUNTER	false	The total number of (interval) cancel_rcvd.	true
BYE_SENT	COUNTER	false	The total number of (interval) bye_sent.	true
BYE_RCVD	COUNTER	false	The total number of (interval) bye_rcvd.	true
INV200_SENT	COUNTER	false	The total number of (interval) inv200_sent.	true
INV200_RCVD	COUNTER	false	The total number of (interval) inv200_rcvd.	true
INV380_SENT	COUNTER	false	The total number of (interval) inv380_sent.	true
INV380_RCVD	COUNTER	false	The total number of (interval) inv380_rcvd.	true
INV400_SENT	COUNTER	false	The total number of (interval) inv400_sent.	true
INV400_RCVD	COUNTER	false	The total number of (interval) inv400_rcvd.	true
INV403_SENT	COUNTER	false	The total number of (interval) inv403_sent.	true
INV403_RCVD	COUNTER	false	The total number of (interval) inv403_rcvd.	true
INV404_SENT	COUNTER	false	The total number of (interval) inv404_sent.	true
INV404_RCVD	COUNTER	false	The total number of (interval) inv404_rcvd.	true
INV406_SENT	COUNTER	false	The total number of (interval) inv406_sent.	true

Column Name	Column Type	Index	Description	canAggregate
INV406_RCVD	COUNTER	false	The total number of (interval) inv406_rcvd.	true
INV408_SENT	COUNTER	false	The total number of (interval) inv408_sent.	true
INV408_RCVD	COUNTER	false	The total number of (interval) inv408_rcvd.	true
INV410_SENT	COUNTER	false	The total number of (interval) inv410_sent.	true
INV410_RCVD	COUNTER	false	The total number of (interval) inv410_rcvd.	true
INV420_SENT	COUNTER	false	The total number of (interval) inv420_sent.	true
INV420_RCVD	COUNTER	false	The total number of (interval) inv420_rcvd.	true
INV480_SENT	COUNTER	false	The total number of (interval) inv480_sent.	true
INV480_RCVD	COUNTER	false	The total number of (interval) inv480_rcvd.	true
INV481_SENT	COUNTER	false	The total number of (interval) inv481_sent.	true
INV481_RCVD	COUNTER	false	The total number of (interval) inv481_rcvd.	true
INV482_SENT	COUNTER	false	The total number of (interval) inv482_sent.	true
INV482_RCVD	COUNTER	false	The total number of (interval) inv482_rcvd.	true
INV483_SENT	COUNTER	false	The total number of (interval) inv483_sent.	true
INV483_RCVD	COUNTER	false	The total number of (interval) inv483_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
INV484_SENT	COUNTER	false	The total number of (interval) inv484_sent.	true
INV484_RCVD	COUNTER	false	The total number of (interval) inv484_rcvd.	true
INV486_SENT	COUNTER	false	The total number of (interval) inv486_sent.	true
INV486_RCVD	COUNTER	false	The total number of (interval) inv486_rcvd.	true
INV487_SENT	COUNTER	false	The total number of (interval) inv487_sent.	true
INV487_RCVD	COUNTER	false	The total number of (interval) inv487_rcvd.	true
INV488_SENT	COUNTER	false	The total number of (interval) inv488_sent.	true
INV488_RCVD	COUNTER	false	The total number of (interval) inv488_rcvd.	true
INV500_SENT	COUNTER	false	The total number of (interval) inv500_sent.	true
INV500_RCVD	COUNTER	false	The total number of (interval) inv500_rcvd.	true
INV501_SENT	COUNTER	false	The total number of (interval) inv501_sent.	true
INV501_RCVD	COUNTER	false	The total number of (interval) inv501_rcvd.	true
INV502_SENT	COUNTER	false	The total number of (interval) inv502_sent.	true
INV502_RCVD	COUNTER	false	The total number of (interval) inv502_rcvd.	true
INV503_SENT	COUNTER	false	The total number of (interval) inv503_sent.	true

Column Name	Column Type	Index	Description	canAggregate
INV503_RCVD	COUNTER	false	The total number of (interval) inv503_rcvd.	true
INV504_SENT	COUNTER	false	The total number of (interval) inv504_sent.	true
INV504_RCVD	COUNTER	false	The total number of (interval) inv504_rcvd.	true
INV580_SENT	COUNTER	false	The total number of (interval) inv580_sent.	true
INV580_RCVD	COUNTER	false	The total number of (interval) inv580_rcvd.	true
INV602_SENT	COUNTER	false	The total number of (interval) inv602_sent.	true
INV602_RCVD	COUNTER	false	The total number of (interval) inv602_rcvd.	true
INV603_SENT	COUNTER	false	The total number of (interval) inv603_sent.	true
INV603_RCVD	COUNTER	false	The total number of (interval) inv603_rcvd.	true
INV606_SENT	COUNTER	false	The total number of (interval) inv606_sent.	true
INV606_RCVD	COUNTER	false	The total number of (interval) inv606_rcvd.	true
INVUNKNOWN_SENT	COUNTER	false	The total number of (interval) invUnknown_sent.	true
INVUNKNOWN_RCV D	COUNTER	false	The total number of (interval) invUnknown_rcvd.	true
NON_INV200_SENT	COUNTER	false	The total number of (interval) nonInv200_sent.	true
NON_INV200_RCVD	COUNTER	false	The total number of (interval) nonInv200_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INV380_SENT	COUNTER	false	The total number of (interval) nonInv380_sent.	true
NON_INV380_RCVD	COUNTER	false	The total number of (interval) nonInv380_rcvd.	true
NON_INV400_SENT	COUNTER	false	The total number of (interval) nonInv400_sent.	true
NON_INV400_RCVD	COUNTER	false	The total number of (interval) nonInv400_rcvd.	true
NON_INV403_SENT	COUNTER	false	The total number of (interval) nonInv403_sent.	true
NON_INV403_RCVD	COUNTER	false	The total number of (interval) nonInv403_rcvd.	true
NON_INV404_SENT	COUNTER	false	The total number of (interval) nonInv404_sent.	true
NON_INV404_RCVD	COUNTER	false	The total number of (interval) nonInv404_rcvd.	true
NON_INV406_SENT	COUNTER	false	The total number of (interval) nonInv406_sent.	true
NON_INV406_RCVD	COUNTER	false	The total number of (interval) nonInv406_rcvd.	true
NON_INV408_SENT	COUNTER	false	The total number of (interval) nonInv408_sent.	true
NON_INV408_RCVD	COUNTER	false	The total number of (interval) nonInv408_rcvd.	true
NON_INV410_SENT	COUNTER	false	The total number of (interval) nonInv410_sent.	true
NON_INV410_RCVD	COUNTER	false	The total number of (interval) nonInv410_rcvd.	true
NON_INV420_SENT	COUNTER	false	The total number of (interval) nonInv420_sent.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INV420_RCVD	COUNTER	false	The total number of (interval) nonInv420_rcvd.	true
NON_INV480_SENT	COUNTER	false	The total number of (interval) nonInv480_sent.	true
NON_INV480_RCVD	COUNTER	false	The total number of (interval) nonInv480_rcvd.	true
NON_INV481_SENT	COUNTER	false	The total number of (interval) nonInv481_sent.	true
NON_INV481_RCVD	COUNTER	false	The total number of (interval) nonInv481_rcvd.	true
NON_INV482_SENT	COUNTER	false	The total number of (interval) nonInv482_sent.	true
NON_INV482_RCVD	COUNTER	false	The total number of (interval) nonInv482_rcvd.	true
NON_INV483_SENT	COUNTER	false	The total number of (interval) nonInv483_sent.	true
NON_INV483_RCVD	COUNTER	false	The total number of (interval) nonInv483_rcvd.	true
NON_INV484_SENT	COUNTER	false	The total number of (interval) nonInv484_sent.	true
NON_INV484_RCVD	COUNTER	false	The total number of (interval) nonInv484_rcvd.	true
NON_INV486_SENT	COUNTER	false	The total number of (interval) nonInv486_sent.	true
NON_INV486_RCVD	COUNTER	false	The total number of (interval) nonInv486_rcvd.	true
NON_INV487_SENT	COUNTER	false	The total number of (interval) nonInv487_sent.	true
NON_INV487_RCVD	COUNTER	false	The total number of (interval) nonInv487_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INV488_SENT	COUNTER	false	The total number of (interval) nonInv488_sent.	true
NON_INV488_RCVD	COUNTER	false	The total number of (interval) nonInv488_rcvd.	true
NON_INV500_SENT	COUNTER	false	The total number of (interval) nonInv500_sent.	true
NON_INV500_RCVD	COUNTER	false	The total number of (interval) nonInv500_rcvd.	true
NON_INV501_SENT	COUNTER	false	The total number of (interval) nonInv501_sent.	true
NON_INV501_RCVD	COUNTER	false	The total number of (interval) nonInv501_rcvd.	true
NON_INV502_SENT	COUNTER	false	The total number of (interval) nonInv502_sent.	true
NON_INV502_RCVD	COUNTER	false	The total number of (interval) nonInv502_rcvd.	true
NON_INV503_SENT	COUNTER	false	The total number of (interval) nonInv503_sent.	true
NON_INV503_RCVD	COUNTER	false	The total number of (interval) nonInv503_rcvd.	true
NON_INV504_SENT	COUNTER	false	The total number of (interval) nonInv504_sent.	true
NON_INV504_RCVD	COUNTER	false	The total number of (interval) nonInv504_rcvd.	true
NON_INV580_SENT	COUNTER	false	The total number of (interval) nonInv580_sent.	true
NON_INV580_RCVD	COUNTER	false	The total number of (interval) nonInv580_rcvd.	true
NON_INV602_SENT	COUNTER	false	The total number of (interval) nonInv602_sent.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INV602_RCVD	COUNTER	false	The total number of (interval) nonInv602_rcvd.	true
NON_INV603_SENT	COUNTER	false	The total number of (interval) nonInv603_sent.	true
NON_INV603_RCVD	COUNTER	false	The total number of (interval) nonInv603_rcvd.	true
NON_INV606_SENT	COUNTER	false	The total number of (interval) nonInv606_sent.	true
INV606_RCVD	COUNTER	false	The total number of (interval) nonInv606_rcvd.	true
NON_INVUNKNOWN_SENT	COUNTER	false	The total number of (interval) nonInvUnknown_sent.	true
NON_INVUNKNOWN_RCVD	COUNTER	false	The total number of (interval) nonInvUnknown_rcvd.	true
CE_NAME	STRING	No	The name of the compute element for this entity.	False

SBCCORESipTGResIntStats

Column name	Column type	Index	Description	canAggregate
ACNAME	STRING	True	The name of this Address Context.	False
ZNAME	STRING	True	The name of this Zone.	False
NAME	STRING	True	The name of this SIP trunk group.	False
DIRECTION	STRING	True	The direction of (Interval) SIP response messages.	False
RESCODE	INTEGER	True	The response code of (Interval) SIP response messages.	False
RESCOUNT	INTEGER	False	The total number of (Interval) SIP response messages for the specified response code.	True

Column name	Column type	Index	Description	canAggregate
CE_NAME	STRING	No	The name of the compute element for this entity.	False

SBCCORETGAggregatedStats

Column Name	Column Type	Index	canAggregate
DIRECTION	STRING	True	False
RESCODE	INTEGER	True	False
RESCOUNT	COUNTER	True	True
CE_NAME	STRING	No	False

SBX5K Stats

SBX5KAclOffListIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SBX5KAggregateOffIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.		

SBX5KArpOffListIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	No	The source IP port of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SBX5KBadEtherIpHdrOffIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
ETHER_TYPE	INTEGER	No	The first ether type found in the Ethernet packet.	True	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SBX5KDiscardRuleOffIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SBX5KDtlsSrtpStats

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	The name of the compute element for this entry.	DTLS Profile - CLI
CURRENT_CLIENT_CONNECTIONS	INTEGER	No	Number of client sessions currently active.	

Column Name	Column Type	Index	Description	CLI Command Reference
CURRENT_SERVER_CONNECTIONS	INTEGER	No	Number of server sessions currently active.	
TOTAL_CLIENT_SESSIONS	INTEGER	No	Cumulative total number of client sessions.	
TOTAL_SERVER_SESSIONS	INTEGER	No	Cumulative total number of server sessions.	
SUCCESSFUL_CLIENT_HANDSHAKES	INTEGER	No	Number of successful client handshakes.	
SUCCESSFUL_SERVER_HANDSHAKES	INTEGER	No	Number of successful server handshakes.	
SESSION_RESUMPTIONS	INTEGER	No	Number of server sessions that resume.	
NO_CIPHER_SUITE	INTEGER	No	Number of handshake failures due to inability to converge on a cipher suite.	
HANDSHAKE_TIMEOUTS	INTEGER	No	Number of handshakes that timed out before completing.	
CLIENT_AUTH_FAILURES	INTEGER	No	Number of times peer failed DTLS authentication with SBC as the client.	
SERVER_AUTH_FAILURES	INTEGER	No	Number of times peer failed DTLS authentication with SBC as the server.	
FATAL_ALERTS_RECEIVED	INTEGER	No	Number of FATAL Alerts received.	
WARNING_ALERTS_RECEIVED	INTEGER	No	Number of WARNING Alerts received.	
HANDSHAKE_FAILURES	INTEGER	No	Cumulative total of all handshake failures.	

Column Name	Column Type	Index	Description	CLI Command Reference
RECEIVE_FAILURES	INTEGER	No	Number of receive failures (failure to decrypt).	
SEND_FAILURES	INTEGER	No	Number of send failures (failure to encrypt).	
NO_CLIENT_CERT	INTEGER	No	Number times we were the client and we failed to derive a certificate to send the server.	
VERSION_MISMATCH	INTEGER	No	Number of failed version MisMatch.	
FINGERPRINT_MISMATCH	INTEGER	No	FingerPrint MisMatch	
NO_SRTP_PROFILE	INTEGER	No	No Srtp Profile.	

SBX5KEthernetPortPacketPortStatus

Column Name	Column Type	Index	Description	canAggregate
AVG_RX_ACTUAL_BW	GAUGE	False	Tracks the Average Incoming Bandwidth used during KPI bin interval in bytes/sec.	Master Trunk Group - CLI
AVG_TX_ACTUAL_BW	GAUGE	False	Tracks the Average Outgoing Bandwidth used during KPI bin interval in bytes/sec.	
PEAK_RX_ACTUAL_BW	GAUGE	False	Tracks the Peak Incoming Bandwidth used during KPI bin interval in bytes/sec.	
PEAK_TX_ACTUAL_BW	GAUGE	False	Tracks the Peak Outgoing Bandwidth used during KPI bin interval in bytes/sec.	
AVG_RX_ACTUAL_BWUTIL	GAUGE	False	Tracks the average incoming BW utilization based on total available port BW instead of negotiated BW.	
PEAK_RX_ACTUAL_BWUTIL	GAUGE	False	Tracks the maximum incoming BW utilization during the KPI bin interval expressed as a percentage of the available BW.	

Column Name	Column Type	Index	Description	canAggregate
AVG_TX_ACTUAL_BWUTIL	GAUGE	False	Tracks the average outgoing BW utilization during the KPI bin interval based on total available BW instead of negotiated BW.	
PEAK_TX_ACTUAL_BWUTIL	GAUGE	False	Tracks the maximum outgoing BW utilization during the KPI bin interval expressed as a percentage of the available BW.	
BWALARM_THRESHOLD_EXCEEDED	GAUGE	False	Tracks the total number of times the BW alarm threshold was passed in the upward direction during the bin interval	
BWALARM_CLEARED	GAUGE	False	Tracks the total number of times the BW clear alarm threshold was passed in the downward direction during the bin interval.	
AVG_USAGE_BW	GAUGE	False	Tracks the Average Bandwidth Usage during KPI bin interval	
PEAK_USAGE_BW	GAUGE	False	Tracks the Peak Bandwidth Usage during KPI bin interval.	
CE_NAME	STRING	True	The host name of the server.	
PORT_NAME	STRING	True	The name of this port.	
NEGOTIATED_SPEED	INTEGER	False	The interface speed. Packet port speed is not negotiable.	
LINK_STATE	INTEGER	False	The state of the interface.	
MAX_BANDWIDTH	GAUGE	False	Maximum bandwidth this port can support, bytes/sec.	
ALLOCATED_BANDWIDTH	GAUGE	False	Bandwidth the active media streams on this port reserve, bytes/sec.	
RX_BANDWIDTH	GAUGE	False	Actual Rx bandwidth in use on this port, bytes/sec.	
TX_BANDWIDTH	GAUGE	False	Actual Tx bandwidth in use on this port, bytes/sec.	

Column Name	Column Type	Index	Description	canAggregate
BANDWIDTH_USAGE	GAUGE	False	Percentage of maximum bandwidth allocated on this port.	
BANDWIDTH_DEVIATION	GAUGE	False	Percentage of deviation of actual bandwidth from the allocated bandwidth.	
MAC_ADDRESS	STRING	False	The MAC address of the network interface.	
IF_INDEX	GAUGE	False	The unique ifIndex of this Packet NIF.	

SBX5KIpSecDecryptOffIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
DEST_IP_PORT	INTEGER	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SBX5KLicenseUsageStats

Name	Type	Index	Description	canAggregate
LICENSE_MODE	STRING	False	Displays the licensing mode of SBC Core.	False
ENCRYPT_ENABLED	INTEGER	False	Set based on whether encrypt license is available at the SBC Core.	False
SRTP_ENABLED	INTEGER	False	Set based on whether srtp license is available at the SBC Core.	False
VIDEO_ENABLED	INTEGER	False	Set based on whether video license is available at the SBC Core.	False
AMRNB_ENABLED	INTEGER	False	Set based on whether amrnb license is available at the SBC Core.	False
AMRWB_ENABLED	INTEGER	False	Set based on whether amrwb license is available at the SBC Core.	False

Name	Type	Index	Description	canAggregate
EVRC_ENABLED	INTEGER	False	Set based on whether evrc license is available at the SBC Core.	False
NICE_ENABLED	INTEGER	False	Set based on whether nicerec license is available at the SBC Core.	False
MRF_ENABLED	INTEGER	False	Set based on whether mrf license is available at the SBC Core.	False
SIPREC_ENABLED	INTEGER	False	Set based on whether siprec license is available at the SBC Core.	False
VDSPRTU_ENABLED	INTEGER	False	Set based on whether transcode license is available at the SBC Core.	False
PDCS_ENABLED	INTEGER	False	Set based on whether pdcs license is available at the SBC Core.	False
LI_ENABLED	INTEGER	False	Set based on whether LI license is available at the SBC Core.	False
RTU_ENABLED	INTEGER	False	Set based on whether SBC Core-RTU license is available at the SBC Core.	False
DSPG722_ENABLED	INTEGER	False	Set based on whether DSPG722license is available at the SBC Core.	False
GMP4X1_ENABLED	INTEGER	False	Set based on whether GMP4X1 license is available at the SBC Core.	False
SIPI_ENABLED	INTEGER	False	Set based on whether SIPI license is available at the SBC Core.	False
SIP323_ENABLED	INTEGER	False	Set based on whether SIP323 license is available at the SBC Core.	False

Name	Type	Index	Description	canAggregate
GMP1X10_ENABLED	INTEGER	False	Set based on whether 1X10GMP license is available at the SBC Core.	False
POLRTU_ENABLED	INTEGER	False	Set based on whether POLRTU license is available at the SBC Core.	False
PSXRTU_ENABLED	INTEGER	False	Set based on whether PSXRTU license is available at the SBC Core.	False
CAPACITY_ENABLED	INTEGER	False	Set based on whether CAPACITY license is available at the SBC Core.	False
E911_ENABLED	INTEGER	False	Set based on whether E911 license is available at the SBC Core.	False
ENUM_ENABLED	INTEGER	False	Set based on whether ENUM license is available at the SBC Core.	False
SWINSTANCE_ENABLED	INTEGER	False	Set based on whether SWINSTANCE license is available at the SBC Core.	False
LBINSTANCE_ENABLED	INTEGER	No	Set based on whether SLB license is available at the SLB.	False
SLBSESS_ENABLED	INTEGER	No	Set based on whether SLB sessions license is available at the SBC.	False
MEDIA_PROBE_AUTH	INTEGER	False	Set based on whether MEDIA PROBE license is available at the SBC.	False
WEB_SOCKET_AUTH	INTEGER	False	Set based on whether WEB SOCKET license is available at the SBC	False
CE_NAME	STRING	No	The name of the compute element for this entity.	False

SBX5KMediaOffIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
ETHER_TYPE	COUNTER	No	The first ether type found in the Ethernet packet.	True	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SBX5KMtrmConnPortPeerStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Zone - MTRM Conn Port - CLI
ZNAME	STRING	Yes	The name of the address context zone.	
STAT_INDEX	GAUGE	Yes	Master Trunk Group Connection Port index.	
PEER_INDEX	INTEGER	Yes	Peer connection index.	
RTO	INTEGER	No	The current Retransmission Time Out in seconds. The messages that are in the retransmission buffer send at this interval.	
IRRT_BUFFER_DEPTH	INTEGER	No	This infinite retry retransmission buffer. The messages in this buffer attempt to send to the peer as long as the connection is alive. If the connection to the peer is lost this buffer is flushed.	

Column Name	Column Type	Index	Description	CLI Command Reference
FRRT_BUFFER_DEPTH	INTEGER	No	The finite retry retransmission buffer. The messages in this buffer attempt to send to the server at most twice. Failure to send this message to the server discards the message. If the connection to the peer is lost this buffer is flushed.	
MSGGS_SENT	INTEGER	No	The total number of messages sent on this port.	
MSGGS_RCVD	INTEGER	No	The total number of messages received on this port.	
SHELF_REG_REQ_MSGGS_SENT	INTEGER	No	The number of Shelf Registration Request messages sent on this port.	
SHELF_REG_REQ_MSGGS_RCVD	INTEGER	No	The number of Shelf Registration Request messages received on this port.	
SHELF_REG_RESPONSE_MSGGS_SENT	COUNTER	No	The number of Shelf Registration Response messages sent on this port.	
SHELF_REG_RESPONSE_MSGGS_RCVD	COUNTER	No	The number of Shelf Registration Response messages received on this port.	
HEALTH_CHECK_REQ_MSGGS_SENT	COUNTER	No	The number of Health Check messages sent from this port.	
HEALTH_CHECK_REQ_MSGGS_RCVD	COUNTER	No	The number of Health Check Request messages received on this port.	

Column Name	Column Type	Index	Description	CLI Command Reference
HEALTH_CHECK_RESP_MSGS_SENT	COUNTER	No	The number of Health Check Response messages sent on this port.	
HEALTH_CHECK_RESP_MSGS_RCVD	COUNTER	No	The number of Health Check Response messages received on this port.	
MTRG_REG_REQ_MSGS_SENT	COUNTER	No	The number of MTRG Reg Request messages sent from this port.	
MTRG_REG_REQ_MSGS_RCVD	COUNTER	No	The number of MTRG Reg Request messages received on this port.	
MTRG_REG_RESP_MSGS_SENT	COUNTER	No	The number of MTRG Reg Response messages sent on this port.	
MTRG_REG_RESP_MSGS_RCVD	COUNTER	No	The number of MTRG Reg Response messages received on this port.	
IP_AUDIT_REQ_MSGS_SENT	COUNTER	No	The number of IP AuditReg Request messages sent from this port.	
IP_AUDIT_REQ_MSGS_RCVD	COUNTER	No	The number of IP Audit Request messages received on this port.	
IP_AUDIT_RESP_MSGS_SENT	COUNTER	No	The number of IP Audit Response messages sent on this port.	
IP_AUDIT_RESP_MSGS_RCVD	COUNTER	No	The number of IP Audit Response messages received on this port.	
BW_ALLOC_REQ_MSGS_SENT	COUNTER	No	The number of BW Alloc Request messages sent from this port.	

Column Name	Column Type	Index	Description	CLI Command Reference
BW_ALLOC_REQ_MSGS_RCVD	COUNTER	No	The number of BW Alloc Request messages received on this port.	
BW_ALLOC_RESP_MSGS_SENT	COUNTER	No	The number of BW Alloc Response messages sent on this port.	
BW_ALLOC_RESP_MSGS_RCVD	COUNTER	No	The number of BW Alloc Response messages received on this port.	
CALL_ALLOC_REQ_MSGS_SENT	COUNTER	No	The number of Call Alloc Request messages sent from this port.	
CALL_ALLOC_REQ_MSGS_RCVD	COUNTER	No	The number of Call Alloc Request messages received on this port.	
CALL_ALLOC_RESP_MSGS_SENT	COUNTER	No	The number of Call Alloc Response messages sent on this port.	
CALL_ALLOC_RESP_MSGS_RCVD	COUNTER	No	The number of Call Alloc Response messages received on this port.	
BW_FREE_REQ_MSGS_SENT	COUNTER	No	The number of BW Free Request messages sent from this port.	
BW_FREE_REQ_MSGS_RCVD	COUNTER	No	The number of BW Free Request messages received on this port.	
CALL_FREE_REQ_MSGS_SENT	COUNTER	No	The number of Call Free Request messages sent from this port.	
CALL_FREE_REQ_MSGS_RCVD	COUNTER	No	The number of Call Free Request messages received on this port.	

Column Name	Column Type	Index	Description	CLI Command Reference
TAKE_BACK_BW_IND_MSGS_SENT	COUNTER	No	The number of Takeback Bandwidth Indication messages sent from this port.	
TAKE_BACK_BW_IND_MSGS_RCVD	COUNTER	No	The number of Takeback Bandwidth Indication messages received on this port.	
TAKE_BACK_CALLS_IND_MESSAGES_SENT	COUNTER	No	The number of Takeback Call Indication messages sent from this port.	
TAKE_BACK_CALLS_IND_MESSAGES_RCVD	COUNTER	No	The number of Takeback Call Indication messages received on this port.	
MTRG_DEREG_REQ_MESSAGES_SENT	COUNTER	No	The number of MTRG Dereg Request messages sent from this port.	
MTRG_DEREG_REQ_MESSAGES_RCVD	COUNTER	No	The number of MTRG Dereg Request messages received on this port.	
MTRG_UNAVAILABLE_MESSAGES_SENT	COUNTER	No	The number of MTRG Unavailable messages sent from this port.	
MTRG_UNAVAILABLE_MESSAGES_RCVD	COUNTER	No	The number of MTRG Unavailable messages received on this port.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

SBX5KRogueMediaIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
ETHER_TYPE	INTEGER	No	The first ether type found in the Ethernet packet.	True	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	
RING_TYPE	INTEGER	No	The media ring type.	False	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SOURCE_UNIQUE	INTEGER	No	Determines if all discards were from a unique source address.	False	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SBX5KSipByeResponseIntervalStats

Name	Type	Index	Description	canAggregate
ACNAME	STRING	True	The name of the address context.	False
ZNAME	STRING	True	The name of the address context.	False
NAME	STRING	True	The name of this SIP peer group.	False
BYE_RESPONSE_401	COUNTER	false	Indicates the total number of (interval) 401 responses for received Bye messages.	True
BYE_RESPONSE_403	COUNTER	false	Indicates the total number of (interval) 403 responses for received Bye messages.	True
BYE_RESPONSE_407	COUNTER	false	Indicates the total number of (interval) 407 responses for received Bye messages.	True
BYE_RESPONSE_481	COUNTER	false	Indicates the total number of (interval) 481 responses for received Bye messages.	True
CE_NAME	STRING	No	The name of the compute element for this entity.	False

SBX5KSipInviteResponseIntervalStats

Name	Index	Type	Description	CanAggregate
ACNAME	True	STRING	The name of the address context.	False

Name	Index	Type	Description	CanAggregate
ZNAME	True	STRING	The name of the address context.	False
NAME	True	STRING	The name of this SIP peer group.	False
INV_RESPONSE_401	False	COUNTER	Indicates the total number of (interval) 401 responses for received Invite messages.	True
INV_RESPONSE_403	False	COUNTER	Indicates the total number of (interval) 403 responses for received Invite messages.	True
INV_RESPONSE_407	False	COUNTER	Indicates the total number of (interval) 407 responses for received Invite messages.	True
INV_RESPONSE_481	False	COUNTER	Indicates the total number of (interval) 481 responses for received Invite messages.	True
CE_NAME	No	STRING	The name of the compute element for this entity.	False

SBX5KSipIpPeerIntervalStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	IP Policing - CLI
ZNAME	STRING	Yes	The name of the address context.	False	
NAME	STRING	Yes	The name of this SIP peer group.	False	
INBOUND_SESSIONS	COUNTER	False	Indicates the total number of (interval) calls routed to this peer.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
INBOUND_CPS	COUNTER	False	Indicates the total number of (interval) calls routed to this peer per second.	True	
TOTAL_INBOUND_SESSIONS	COUNTER	False	Indicates the total number of (interval) inbound active sessions.	True	
OUTBOUND_SESSIONS	COUNTER	False	Indicates the total number of (interval) calls initiated by this peer.	True	
OUTBOUND_CPS	COUNTER	False	Indicates the total number of (interval) calls initiated by this peer per second.	True	
TOTAL_OUTBOUND_SESSIONS	COUNTER	False	Indicates the total number of (interval) outbound active sessions.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SBX5KSipOptResponseIntervalStats

Name	Index	Type	Description	canAggregate
ACNAME	True	STRING	The name of the address context.	False
ZNAME	True	STRING	The name of the address context.	False
NAME	True	STRING	The name of this SIP peer group.	False
OPT_RESPONSE_401	False	COUNTER	Indicates the total number of (interval) 401 responses for received Option messages.	True

Name	Index	Type	Description	canAggregate
OPT_RESPONSE_403	False	COUNTER	Indicates the total number of (interval) 403 responses for received Option messages.	True
OPT_RESPONSE_407	False	COUNTER	Indicates the total number of (interval) 407 responses for received Option messages.	True
OPT_RESPONSE_481	False	COUNTER	Indicates the total number of (interval) 481 responses for received Option messages.	True
CE_NAME	No	STRING	The name of the compute element for this entity.	False

SBX5KSipRegResponseIntervalStats

Name	Index	Type	Description	canAggregate
ACNAME	True	STRING	The name of the address context.	False
ZNAME	True	STRING	The name of the address context.	False
NAME	True	STRING	The name of this SIP peer group.	False
REG_RESPONSE_401	False	COUNTER	Indicates the total number of (interval) 401 responses for received Register messages.	True
REG_RESPONSE_403	False	COUNTER	Indicates the total number of (interval) 403 responses for received Register messages.	True
REG_RESPONSE_407	False	COUNTER	Indicates the total number of (interval) 407 responses for received Register messages.	True
REG_RESPONSE_481	False	COUNTER	Indicates the total number of (interval) 481 responses for received Register messages.	True
CE_NAME	No	STRING	The name of the compute element for this entity.	False

SBX5KSrtpDecryptOffIntStat

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	No	The source IP address of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	INTEGER	No	The destination IP port of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
ETHER_TYPE	INTEGER	No	The first ether type found in the Ethernet packet.	True	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SOURCE_UNIQUE	INTEGER	No	Determines if all discards were from a unique source address.	False	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SBX5KSystemDspStatusDspUsageStats

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
SYSTEM_NAME	STRING	True	Name of the system.		Show Status System

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
COMPRESSION_TOTAL	INTEGER	False	Total compression resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
COMPRESSI ON_UTILIZATI ON	INTEGER	False	Percentage utilization of compression resources on this server.		
COMPRESSI ON_ALLOC_F AILURES	INTEGER	False	Percentage of compression resources allocation failures on this server.		
G711_TOTAL	INTEGER	False	Total G711 resource capacity on this server.		
G711_UTILIZ ATION	INTEGER	False	Percentage utilization of G711 resources on this server.		
G726_TOTAL	INTEGER	False	Total G726 resource capacity on this server.		
G726_UTILIZ ATION	INTEGER	False	Percentage utilization of G726 resources on this server.		
G729AB_TOT AL	INTEGER	False	Total G729A+B resource capacity on this server.		
G729AB_UTIL IZATION	INTEGER	False	Percentage utilization of G729A+B resources on this server.		
G7231_TOTA L	INTEGER	False	Total G723.1 resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G7231_UTILIZATION	INTEGER	False	Percentage utilization of G7231 resources on this server.		
ILBC_TOTAL	INTEGER	False	Total iLBC resource capacity on this server.		
ILBC_UTILIZATION	INTEGER	False	Percentage utilization of iLBC resources on this server.		
ILBC_ALLOC_FAILURES	INTEGER	False	Percentage of iLBC resources allocation failures on this server.		
ECM_TOTAL	INTEGER	False	Total T.38 ECM resource capacity on this server.		
ECM_UTILIZATION	INTEGER	False	Percentage utilization of T.38 ECM resources on this server.		
ECM_ALLOC_FAILURES	INTEGER	False	Percentage of T.38 ECM resources allocation failures on this server.		
TONE_TOTAL	INTEGER	False	Total tone resource capacity on this server.		
TONE_UTILIZATION	INTEGER	False	Percentage utilization of tone resources on this server.		
TONE_ALLOC_FAILURES	INTEGER	False	Percentage of tone resource allocation failures on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
EVRCB0_TOTAL	INTEGER	False	Total EVRCB0 resource capacity on this server.		
EVRCB0_UTILIZATION	INTEGER	False	Percentage utilization of EVRCB0 resources on this server.		
EVRCB0_ALL_OC_FAILURES	INTEGER	False	Percentage of EVRCB0 resources allocation failures on this server.		
AMRNB_TOTAL	INTEGER	False	Total AMR-NB resource capacity on this server.		
AMRNB_UTILIZATION	INTEGER	False	Percentage utilization of AMR-NB resources on this server.		
AMRNB_ALL_OC_FAILURES	INTEGER	False	Percentage of AMR-NB resources allocation failures on this server.		
AMRWB_TOTAL	INTEGER	False	Total AMR-WB resource capacity on this server.		
AMRWB_UTILIZATION	INTEGER	False	Percentage utilization of AMR-WB resources on this server.		
AMRWB_ALL_OC_FAILURES	INTEGER	False	Percentage of AMR-WB resources allocation failures on this server.		
G722_TOTAL	INTEGER	False	Total G.722 resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G722_UTILIZATION	INTEGER	False	Percentage utilization of G.722 resources on this server.		
G722_ALLOC_FAILURES	INTEGER	False	Percentage of G.722 resources allocation failures on this server.		
EVRC0_TOTAL	INTEGER	False	Total EVRC0 resource capacity on this server.		
EVRC0_UTILIZATION	INTEGER	False	Percentage utilization of EVRC0 resources on this server.		
EVRC0_ALLOC_FAILURES	INTEGER	False	Percentage of EVRC0 resources allocation failures on this server.		
COMPRESSION_AVAILABLE	INTEGER	False	Number of compression resources currently unused and available on this server.		
TONE_AVAILABLE	INTEGER	False	Number of tone resources currently unused and available on this server.		
G7221_TOTAL	INTEGER	False	Total G.722.1 resource capacity on this server.		
G7221_UTILIZATION	INTEGER	False	Percentage utilization of G.722.1 resources on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
EFR_TOTAL	INTEGER	False	Total EFR resource capacity on this server.		
EFR_UTILIZATION	INTEGER	False	Percentage utilization of EFR resources on this server.		
G711SS_TOTAL	INTEGER	False	Total G711SS (silence suppression) resource capacity on this server.		
G711SS_UTILIZATION	INTEGER	False	Percentage utilization of G711SS (silence suppression) resources on this server.		
SLOT1_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
SLOT2_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
SLOT3_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
SLOT4_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
G711V8_TOTAL	INTEGER	False	Total G711 V8 resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711V8_UTILIZATION	INTEGER	False	Percentage utilization of G711 V8 resources on this server.		
G711SSV8_TOTAL	INTEGER	False	Total G711SS (silence suppression) V8 resource capacity on this server.		
G711SSV8_UTILIZATION	INTEGER	False	Percentage utilization of G711SS (silence suppression) V8 resources on this server.		
G726V8_TOTAL	INTEGER	False	Total G726 V8 resource capacity on this server.		
G726V8_UTILIZATION	INTEGER	False	Percentage utilization of G726 V8 resources on this server.		
G7231V8_TOTAL	INTEGER	False	Total G723.1 V8 resource capacity on this server.		
G7231V8_UTILIZATION	INTEGER	False	Percentage utilization of G7231 V8 resources on this server.		
G722V8_TOTAL	INTEGER	False	Total G.722 V8 resource capacity on this server.		
G722V8_UTILIZATION	INTEGER	False	Percentage utilization of G.722 V8 resources on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G7221V8_TOTAL	INTEGER	False	Total G.722.1 V8 resource capacity on this server.		
G7221V8_UTILIZATION	INTEGER	False	Percentage utilization of G.722.1 V8 resources on this server.		
G729ABV8_TOTAL	INTEGER	False	Total G729A+B V8 resource capacity on this server.		
G729ABV8_UTILIZATION	INTEGER	False	Percentage utilization of G729A+B V8 resources on this server.		
ECMV34_TOTAL	INTEGER	False	Total T.38 ECM V.34 resource capacity on this server.		
ECMV34_UTILIZATION	INTEGER	False	Percentage utilization of T.38 ECM V.34 resources on this server.		
ILBCV8_TOTAL	INTEGER	False	Total iLBC V8 resource capacity on this server.		
ILBCV8_UTILIZATION	INTEGER	False	Percentage utilization of iLBC V8 resources on this server.		
OPUS_TOTAL	INTEGER	False	Total OPUS resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
OPUS_UTILIZATION	INTEGER	False	Percentage utilization of OPUS resources on this server.		
OPUS_ALLOC_FAILURES	INTEGER	False	Percentage of OPUS resources allocation failures on this server.		
USAGE_SILK8_TOTAL	COUNT	False	Total SILK_8 resource capacity on the present server.		
USAGE_SILK8_UTILIZATION	COUNT	False	Percentage utilization of SILK_8 resources on the present server.		
USAGE_SILK16_TOTAL	COUNT	False	Total SILK_16 resource capacity on the present server		
USAGE_SILK16_UTILIZATION	COUNT	False	The utilization percentage of SILK_16 resources on the present server		
USAGE_AMRNB_T140_TOTAL	INTEGER	true	Total AMR-NB with T.140 resource capacity in the server.		
USAGE_AMRNB_T140_UTILIZATION	INTEGER	False	The utilization percentage of AMR-NB with T.140 resource in the server.		
USAGE_AMRWB_T140_TOTAL	INTEGER	False	Total AMR-WB with T.140 resource capacity in the server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
USAGE_AMR_WBT140_UTILIZATION	INTEGER	False	The utilization percentage of AMR-WB with T.140 resource in the server.		
COMP_HP_UTILIZATION	INTEGER	False	Percentage utilization of AMR-WB with T.140 resource on this server.		
RESOURCE_HP_UTILIZATION	INTEGER	False	Percentage utilization of tone resources used for high priority calls on this server.		
DSP_EVS_T140_TOTAL	INTEGER	False	Total EVS with T.140 resource capacity on this server.		
DSP_EVS_T140_UTILIZATION	INTEGER	False	Percentage utilization of EVS with T.140 resources on this server		
G711T140_TOTAL	GAUGE	False	The total G711 with T.140 resource capacity on this server.	MEAN	
G711T140_UTILIZATION	GAUGE	False	The percentage utilization of G711 with T.140 resources on this server.	MEAN	
G711SST140_TOTAL	GAUGE	False	The total G711SS with T.140 resource capacity on this server.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SST140_UTILIZATION	GAUGE	False	The percentage utilization of G711SS with T.140 resources on this server.	MEAN	
OPUST140_TOTAL	GAUGE	False	The total Opus with T.140 resource capacity on this server.	MEAN	
OPUST140_UTILIZATION	GAUGE	False	The percentage utilization of Opus with T.140 resources on this server.	MEAN	
G722T140_TOTAL	GAUGE	False	The total G722 with T.140 resource capacity on this server.	MEAN	
G722T140_UTILIZATION	GAUGE	False	The percentage utilization of G722 with T.140 resources on this server.	MEAN	
G722V8T140_TOTAL	GAUGE	False	The total G722 V8 with T.140 resource capacity on this server.	MEAN	
G722V8T140_UTILIZATION	GAUGE	False	The percentage utilization of G722 V8 with T.140 resources on this server.	MEAN	
G711V8T140_TOTAL	GAUGE	False	The total G711 V8 with T.140 resource capacity on this server.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711V8T140_UTILIZATION	GAUGE	False	The percentage utilization of G711 V8 with T.140 resources on this server.	MEAN	
G711SSV8T140_TOTAL	GAUGE	False	The total G711SS V8 with T.140 resource capacity on this server.	MEAN	
G711SSV8T140_UTILIZATION	GAUGE	False	The percentage utilization of G711SS V8 with T.140 resources on this server.	MEAN	
L16_TOTAL	GAUGE	False	The total L16 resource capacity on this server.	MEAN	
L16_UTILIZATION	GAUGE	False	The percentage utilization of L16 resources on this server.	MEAN	
CE_NAME	STRING	False	The name of the compute element for this entity.	N/A	

SBX5KUflowOffListIntStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ROLE	INTEGER	Yes	Role of the system.	False	IP Policing - CLI
SERIAL_INDEX	INTEGER	Yes	The index of the system.	True	
ADDRESS_CONTEXT	STRING	No	The name of the address context of the table entry.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
INTERFACE_GROUP_NAME	STRING	No	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	No	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	No	The source IP port of the table entry.	True	
DEST_IP_ADDRESS	STRING	No	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	No	The source IP port of the table entry.	True	
DEST_IP_PORT	STRING	No	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	No	The IP Protocol of the table entry.	True	
DISCARD_COUNT	COUNTER	No	The number of packets discarded by the policer.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

Shared CAC Stats

SharedCacFailureIntStats

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
NAME	STRING	True	The name of this shared CAC-limits pool.	False	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
ALLOC_FAIL_BW_LIMIT	GAUGE	False	The number of BW Requests which fail because the specified interval of this shared CAC limits pool exceeds the configured bandwidth limit.	True	
ALLOC_FAIL_CALL_LIMIT	GAUGE	False	The number of BW Requests which fail because the specified interval of this shared CAC limits pool exceeds the configured call limit.	False	
ALLOC_FAIL_PARENT_CONSTR	GAUGE	False	The current number of failures because of a parent limit denial for the specified interval.	False	
ALLOC_FAIL_SIP_REG	GAUGE	False	The number of SIP registration attempts that failed because the specified interval of this shared CAC limits pool exceeds the configured registration limit.	False	
SIP_SUB_FAIL_POLICING	GAUGE	False	The current number of SIP Subscribe attempts that failed due to policing on a trunk group.	False	
SIP_OTHER_REQ_FAIL_POLICING	GAUGE	False	The current number of SIP other non-invite attempts that failed due to policing on a trunk group.	False	
VIDEO_THRESHOLD_LIMIT	GAUGE	False	The number of exceeded video threshold limits for this shared CAC limits pool.	False	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SharedCacIntervalStatistics

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
NAME	STRING	True	The name of this shared CAC-limits pool.	False	
MAX_ACTIVE_CALLS	GUAGE	False	The current high watermark of total number of active calls in both the inbound and outbound directions using limits from this shared CAC limits pool.	False	
IN_BW_USAGE	GUAGE	False	The sum of BW usage (expected data rate in bits per second multiplied by call duration in seconds) for every inbound call associated with this shared CAC limits pool for the specified interval.	False	
OUT_BW_USAGE	GUAGE	False	The sum of BW usage (expected data rate in bits per second multiplied by call duration in seconds) for every outbound call associated with this shared CAC limits pool for the specified interval.	False	
MAX_ACTIVE_BW_USAGE	GUAGE	False	The high watermark of BW usage in either direction associated with this shared CAC limits pool for the specified interval.	False	
ACTIVE_REGS	GUAGE	False	The current number of active registrations of this shared CAC-limits pool.	False	
MAX_ACTIVE_REGS	GUAGE	False	The number of maximum active registrations of this shared CAC-limits pool (this is the high-watermark achieved on this pool during this interval).	False	
ACTIVE_SUBS	GUAGE	False	The current number of active subscriptions on this shared CAC-limits pool.	False	
MAX_ACTIVE_SUBS	GUAGE	False	The current number of maximum active subscriptions on this shared CAC-limits pool. (This is the high-watermark achieved on this shared CAC).	False	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SIP Stats

SipIntervalStats

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context.	False	
NAME	STRING	Yes	The name of this SIP peer group.	False	
RCV_INVITE	COUNTER	No	Indicates the total number of (interval) received Invite messages.	False	
SEND_INVITE	COUNTER	No	Indicates the total number of (interval) sent Invite messages.	False	
RCV_ACK	COUNTER	No	Indicates the total number of (interval) Received Ack.	False	
SEND_ACK	COUNTER	No	Indicates the total number of (interval) Sent Ack messages.	False	
RCV_PRACK	COUNTER	No	Indicates the total number of (interval) received Prack messages.	False	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
SND_PRACK	COUNTER	No	Indicates the total number of (interval) sent Prack messages.	False	
RCV_INFO	COUNTER	No	Indicates the total number of (interval) received INFO messages.	False	
SND_INFO	COUNTER	No	Indicates the total number of (interval) sent INFO messages.	False	
RCV_REFER	COUNTER	No	Indicates the total number of (interval) received Refer messages.	False	
SND_REFER	COUNTER	No	Indicates the total number of (interval) sent Refer messages.	False	
RCV_BYE	COUNTER	No	Indicates the total number of (interval) Received Bye messages.	False	
SND_BYE	COUNTER	No	Indicates the total number of (interval) sent Bye messages.	False	
RCV_CANCEL	COUNTER	No	Indicates the total number of (interval) received Cancel messages.	False	
SND_CANCEL	COUNTER	No	Indicates the total number of (interval) sent Cancel messages.	False	
RCV_REGISTER	COUNTER	No	Indicates the total number of (interval) received Register messages.	False	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
SND_REGISTER	COUNTER	No	Indicates the total number of (interval) sent Register messages.	False	
RCV_UPDATE	COUNTER	No	Indicates the total number of (interval) received Update messages.	False	
SND_UPDATE	COUNTER	No	Indicates the total number of (interval) sent Update messages.	False	
RCV18_X	COUNTER	No	Indicates the total number of (interval) received 18x messages.	False	
SND18_X	COUNTER	No	Indicates the total number of (interval) sent 18x messages.	False	
RCV1_XX	COUNTER	No	Indicates the total number of (interval) received 1xx msg except 18x messages.	False	
SND1_XX	COUNTER	No	Indicates the total number of (interval) sent 1xx msg except 18x messages.	False	
RCV2_XX	COUNTER	No	Indicates the total number of (interval) received 2xx(Invite) messages.	False	
SND2_XX	COUNTER	No	Indicates the total number of (interval) sent 2xx(Invite) messages.	False	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
RCV_NON_I NV2_XX	COUNTER	No	Indicates the total number of (interval) received 2xx(NonInvite) messages.	False	
SND_NON_I NV2_XX	COUNTER	No	Indicates the total number of (interval) sent 2xx(NonInvite) messages.	False	
RCV3_XX	COUNTER	No	Indicates the total number of (interval) recieved 3xx messages.	False	
SND3_XX	COUNTER	No	Indicates the total number of (interval) sent 3xx messages.	False	
RCV4_XX	COUNTER	No	Indicates the total number of (interval) received 4xx messages.	False	
SND4_XX	COUNTER	No	Indicates the total number of (interval) sent 4xx messages.	False	
RCV5_XX	COUNTER	No	Indicates the total number of (interval) receive 5xx messages.	False	
SND5_XX	COUNTER	No	Indicates the total number of (interval) sent 5xx messages.	False	
RCV6_XX	COUNTER	No	Indicates the total number of (interval) receive 6xx messages.	False	
SND6_XX	COUNTER	No	Indicates the total number of (interval) sent 6xx messages.	False	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
RCV_NON_I NV_ERR	COUNTER	No	Indicates the total number of (interval) receive Nonlvite Error messages.	False	
SND_NON_I NV_ERR	COUNTER	No	Indicates the total number of (interval) sent Nonlvite Error messages.	False	
RCV_UNKNO WN_MSG	COUNTER	No	Indicates the total number of (interval) receive Unknown messages.	False	
RCV_SUBSC RIBER	COUNTER	No	Indicates the total number of (interval) receive Subscriber messages.	False	
SND_SUBSC RIBER	COUNTER	No	Indicates the total number of (interval) sent Subscriber messages.	False	
RCV_NOTIFY	COUNTER	No	Indicates the total number of (interval) receiveNotify messages.	False	
SND_NOTIFY	COUNTER	No	Indicates the total number of (interval) sent Notify messages.	False	
RCV_OPTIO N	COUNTER	No	Indicates the total number of (interval) receive Option messages.	False	
SND_OPTIO N	COUNTER	No	Indicates the total number of (interval) sent Option messages.	False	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
INV_RE_TRANSMIT	COUNTER	No	Indicates the total number of (interval) Invite messages ReTransmitted.	False	
REG_RE_TRANSMIT	COUNTER	No	Indicates the total number of (interval) Register messages ReTransmitted.	False	
BYE_RETRANSMIT	COUNTER	No	Indicates the total number of (interval) Bye messages ReTransmitted.	False	
CANCEL_RE_TRANSMIT	COUNTER	No	Indicates the total number of (interval) Cancel messages ReTransmitted.	False	
OTHER_RE_TRANSMIT	COUNTER	No	Indicates the total number of (interval) Other messages ReTransmitted.	False	
RCV_MESSAGE	COUNTER	No	Indicates the total number of (interval) received Message method.	False	
SND_MESSAGE	COUNTER	No	Indicates the total number of (interval) sent Message method.	False	
RCV_PUBLISH	COUNTER	No	Indicates the total number of (interval) received Publish method.	False	
SND_PUBLISH	COUNTER	No	Indicates the total number of (interval) sent Publish method.	False	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
EMERGENCY_ACCEPT	COUNTER	No	Indicates the total number of (interval) emergency calls accepted.	False	
EMERGENCY_REJECT_BWCALL	COUNTER	No	Indicates the total number of (interval) emergency calls rejected because of bandwidth limit or call limit.	False	
EMERGENCY_REJECT_PRIORITY	COUNTER	No	Indicates the total number of (interval) emergency calls rejected because of Priority Policer.	False	
HPC_ACCEPT	COUNTER	No	Indicates the total number of (interval) HPC calls accepted.	False	
NUM_OF_CALLS_SENDING_AARS	COUNTER	No	Indicates the number of calls sending AAR requests.	False	
NUM_OF_RECEIVED_AAA_FAILURES	COUNTER	No	Indicates the number of received AAA failures.	False	
NUM_OF_RECEIVED_AAA_SUCCESSES	COUNTER	No	Indicates the number of received AAA Successes.	True	
NUM_OF_TOTAL_AAR_SENT	COUNTER	No	Indicates the total number of AAR messages sent.	False	
NUM_OF_TIMEOUT_OR_ERROR_AAR	COUNTER	No	Indicates the number of AAR messages not answered.	False	
NUM_OF_RECEIVED_RARS	COUNTER	No	Indicates the number of RAR messages received.	True	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
NUM_OF_RECEIVED_ASRS	COUNTER	No	Indicates the number of ASR messages received.	True	
NUM_OF_SENT_STRS	COUNTER	No	Indicates the number of STR messages sent.	True	
EMERGENCY_REG_ACCEPT	COUNTER	No	Indicates the number of (interval) emergency registrations accepted.	False	
EMERGENCY_REG_REJECT_LIMIT	COUNTER	No	Indicates the number of (interval) emergency registrations rejected because of the registration limit.	False	
EMERGENCY_REG_REJECT_POLICER	COUNTER	No	Indicates the number of (interval) emergency registrations rejected because of the Priority Policer.	False	
EMERGENCY_OOD_ACCEPT	COUNTER	No	Indicates the number of (interval) emergency OOD Requests accepted.	True	
EMERGENCY_OOD_REJECT_POLICER	COUNTER	No	Indicates the number of (interval) emergency OOD Requests rejected because of the Priority Policer.	True	
EMERGENCY_SUBSCRIBE_ACCEPT	COUNTER	No	Indicates the number of (interval) emergency Subscribe Requests accepted.	True	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
EMERGENCY_SUBS_REJECT_POLICER	COUNTER	No	Indicates the number of (interval) emergency Subscribe Requests rejected because of the Priority Policer.	True	
EMERGENCY_SUBS_REJECT_LIMIT	COUNTER	No	Indicates the number of (interval) emergency Subscribe Requests rejected because of the subscription limit	True	
PARSE_ERROR	COUNTER	No	Indicates the total number of (interval) Parse Errors.	True	
NUM_OF_TOTAL_UDR_SENT	COUNTER	No	Indicates the total number of UDR messages sent.	True	
NUM_OF_TIMEOUT_UDR_ERROR	COUNTER	No	Indicates the number of UDR messages not answered.	True	
NUM_OF_RECEIVED_UDA_SUCCESS	COUNTER	No	Indicates the number of received UDA success	True	
NUM_OF_RECEIVED_UDA_FAILURE	COUNTER	No	Indicates the number of received UDA failures.	True	
TOTAL_NUM_S8HR_OUT_REG	COUNTER	No	Indicates the total number (includes success and failed) of registration received from S8HR Outbound Roaming Users.	True	
NUM_S8HR_OUT_REG_SUCCESS	COUNTER	No	Indicates the number of successful registration from S8HR Outbound Roaming Users.	True	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
NUM_S8HR_OUT_REG_FAIL	COUNTER	No	Indicates the number of S8HR Outbound Roaming Users's registrations failed.	True	
TOTAL_NUM_S8HR_OT_NML_CALL	COUNTER	No	Indicates the total number of normal calls initiated from S8HR Outbound Roaming Users.	True	
NUM_OF_S8HR_OT_NML_CALL_SUC	COUNTER	No	Indicates the number of successful normal calls from S8HR Outbound Roaming Users.	True	
NUM_OF_S8HR_OT_NML_CALL_FAIL	COUNTER	No	Indicates the total number of failed normal calls from S8HR Outbound Roaming Users.	True	
NUM_OF_S8HR_OT_EMG_CALL_REJ	COUNTER	No	Indicates the number of S8HR Outbound Roaming User's emergency calls rejected.	True	
NUM_OF_S8HR_IN_EMG_REG_SUC	COUNTER	No	Indicates the number of Successful registration from S8HR Inbound Roaming Users.	True	
NUM_OF_S8HR_IN_EMG_REG_FAIL	COUNTER	No	Indicates the number of S8HR Inbound User's registration rejected.	True	
NUM_OF_S8HR_IN_EMG_CALL_SUC	COUNTER	No	Indicates the number of successful emergency calls from S8HR Inbound User.	True	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
NUM_OF_S8 HR_IN_EMG _CALL_FAIL	COUNTER	No	Indicates the number of S8HR Inbound Users emergency calls failed.	True	
NUM_OF_IN_ HPC_CALL_ ACC	INTEGER	No	Indicates the total number of (interval) Ingress HPC calls accepted.	True	
NUM_OF_OU T_HPC_CALL _ACC	INTEGER	No	Indicates the total number of (interval) Egress HPC calls accepted.	True	
NUM_OF_HP C_4XX_MSG _SENT	INTEGER	No	Indicates the total number of (interval) sent HPC 4xx messages.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

sipOcsCallIntervalStatistics

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context zone.	
NAME	STRING	Yes	The name of this SIP trunk group.	
ATTEMPTED_C ALLS	GAUGE	No	Current Attempted OCS Call statistics.	
RELAYED_CALL S	GAUGE	No	Current Relayed OCS Invite to Egress side statistics.	

Column Name	Column Type	Index	Description	CLI Command Reference
ESTABLISHED_CALLS	GAUGE	No	Current Established OCS Call statistics.	
SUCCESSFUL_CALLS	GAUGE	No	Current Successful OCS Call statistics.	
FAILED_CALLS	GAUGE	No	Current Failed OCS Call statistics.	
PENDING_CALL	GAUGE	No	Current Pending OCS Call statistics.	
REJECTED_CALL	GAUGE	No	Current SBX Rejected OCS Call statistics.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

SipIpPeerOptionsIntervalStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
ACNAME	STRING	Yes	The name of the address context.	False	N/A	N/A
ZNAME	STRING	Yes	The name of this Zone.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_NAME	STRING	Yes	The name of this SIP IP Peer.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_DIRECTION	STRING	Yes	Indicates the direction of the (interval) SIP Options/Response messages.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_MESSAGE	STRING	Yes	Indicates the cause code of the (interval) SIP Options/Response messages.	False	N/A	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
SIP_IP_PEER_OPTIONS_MSG_COUNT	COUNTER	No	Indicates the total number of (interval) SIP Options/Response messages for the specified cause code.	True	Sum	N/A
CE_NAME	STRING	No	The name of the compute element for this entity.	False	No	N/A

SipRegCountStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
NAME	INTEGER	Yes	Name of the system.	
SIP_REG_COUNT_ATTEMPTS	COUNTER	No	Indicates the number of SIP registration attempts.	
SIP_REG_COUNT_CUM_COMPLETIONS	COUNTER	No	Indicates the accumulative number of completed SIP registration attempts.	
SIP_REG_COUNT_PENDING	COUNTER	No	Indicates the current number of pending SIP registrations.	
SIP_REG_COUNT_STABLE	COUNTER	No	Indicates the current number of stable SIP registrations.	
SIP_REG_COUNT_TOTAL	COUNTER	No	Indicates the total number of current SIP registrations.	
SIP_EMERGENCY_REG_ACCEPT_TOTAL	COUNTER	No	Indicates the total number of accepted emergency SIP registrations.	

Column Name	Column Type	Index	Description	CLI Command Reference
SIP_EMERGENCY_REG_ACTIVE_TOTAL	COUNTER	No	Indicates the total number of active emergency SIP registrations.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

SipSigConnStatisticsStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	Yes	The name of the address context.	False
ZNAME	STRING	Yes	The name of the address context zone.	False
IND	GAUGE	Yes	The index of this SIP Signaling Port.	False
TCP_CONNECTION	COUNTER	No	Number of current TCP connections	True
TOTAL_TCP_CONNECTION	COUNTER	No	Number of total TCP connections made.	True
ACTIVE_TLS_TCP_CONNECTION	COUNTER	No	Number of current TLS-TCP connections made.	True
TOTAL_TLS_TCP_CONNECTION	COUNTER	No	Number of total TLS-TCP connections.	True
CE_NAME	STRING	No	The name of the compute element for this entity.	False

SipSigPortStatisticsStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context

Column Name	Column Type	Index	Description	CLI Command Reference
ZNAME	STRING	Yes	The name of the address context.	
IND	GAUGE	Yes	The index of this SIP Signaling Port.	
CALL_RATE	INTEGER	No	number of SIP calls per second during the last minute.	
ORIG_CALLS	INTEGER	No	Total number of outgoing calls sent out from this signaling port.	
TERM_CALLS	INTEGER	No	Total number of incoming calls received on this signaling port.	
TX_PDUS	COUNTER64	No	The total number of signaling PDUS sent out on this port.	
RX_PDUS	COUNTER64	No	The total number of signaling PDUS received on this port.	
TX_BYTES	COUNTER64	No	The total number of signaling BYTES sent out from this port.	
RX_BYTES	COUNTER64	No	The total number of signaling BYTES received by this port.	
IN_REGS	INTEGER	No	Total number of inbound registration(s) received on this signaling port.	
OUT_REGS	INTEGER	No	Total number of outbound registration(s) sent on this signaling port.	
TX500S	INTEGER	No	The total number of 500 responses generated by the SLB when it is unable to forward a request.	

Column Name	Column Type	Index	Description	CLI Command Reference
TX503S	INTEGER	No	The total number of 503 responses generated by the SLB when there are no backend SBCs able to handle the request due to the congestion or the cac restrictions.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

Note

SipSigPortTlsStats is not supported from SBC 4.1 onwards.

SipSigPortTlsStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	NA
ZNAME	STRING	Yes	The name of the address context zone.	
IND	GAUGE	Yes	The index of this SIP Signaling Port.	
CURRENT_CLIENT_SESSIONS	INTEGER	No	Number of client sessions currently active.	
CURRENT_SERVER_SESSIONS	INTEGER	No	Number of server sessions currently active.	
CURRENT_SUSPENDED_SESSIONS	INTEGER	No	Number of server sessions currently suspended.	
TOTAL_CLIENT_SESSIONS	INTEGER	No	Cumulative total number of client sessions.	
TOTAL_SERVER_SESSIONS	INTEGER	No	Cumulative total number of server sessions.	

Column Name	Column Type	Index	Description	CLI Command Reference
CURRENT_CLIENT_HANDSHAKES	INTEGER	No	Number of incomplete client handshakes.	
CURRENT_SERVER_HANDSHAKES	INTEGER	No	Number of incomplete server handshakes.	
SESSION_RESUMPTIONS	INTEGER	No	Number of server sessions that resume.	
NO_CIPHER_SUITE	INTEGER	No	Number of handshake failures due to inability to converge on a cipher suite.	
HANDSHAKE_TIMEOUTS	INTEGER	No	Number of handshakes that timed out before completing.	
HIGHER_AUTH_TIMEOUT	INTEGER	No	Number of handshakes in which the SBC was the server and the client did not authenticate itself through TLS and failed to authenticate itself through any higher level protocol (for example, SIP) before timing out.	
CLIENT_AUTH_FAILURES	INTEGER	No	Number of times peer failed TLS authentication with SBC as the client.	
SERVER_AUTH_FAILURES	INTEGER	No	Number of times peer failed TLS authentication with SBC as the server.	
FATAL_ALERTS_RECEIVED	INTEGER	No	Number of FATAL Alerts received.	
WARNING_ALERTS_RECEIVED	INTEGER	No	Number of WARNING Alerts received.	
HANDSHAKE_FAILURES	INTEGER	No	Cumulative total of all handshake failures.	

Column Name	Column Type	Index	Description	CLI Command Reference
RECEIVE_FAILURES	INTEGER	No	Number of receive failures (failure to decrypt).	
SEND_FAILURES	INTEGER	No	Number of send failures (failure to encrypt).	
NO_AUTH_DROPS	INTEGER	No	Number of SIP messages dropped due to lack of peer authentication at the SIP level.	
NO_AUTH488	INTEGER	No	Number of SIP messages rejected with 488 due to lack of peer authentication at the SIP level.	
MID_CONNECTION_HELLO	INTEGER	No	Number times a peer sent a TLS Hello on a connection that was already up (that is, the peer tried to renegotiate.).	
NO_CLIENT_CERT	INTEGER	No	Number times we were the client and we failed to derive a certificate to send the server.	
VALIDATION_FAILURES	INTEGER	No	Number of failed certificate validations.	
CURRENT_CLIENT_CONNECTIONS	INTEGER	No	Current number of client tls connections.	
TOTAL_CLIENT_CONNECTIONS	INTEGER	No	Cumulative total number of client tls connections.	
CURRENT_SERVER_CONNECTIONS	INTEGER	No	Current number of server tls connections.	
TOTAL_SERVER_CONNECTIONS	INTEGER	No	Cumulative total number of server tls connections.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

SipSubCountStats

Column Name	Column Type	Index	Description
ACNAME	STRING	Yes	The name of the address context.
NAME	INTEGER	Yes	Name of the system.
SIP_SUB_COUNT_ATTEMPTS	COUNTER	No	Indicates the number of SIP relayed subscription attempts.
SIP_SUB_COUNT_CUM_COMPLETIONS	COUNTER	No	Indicates the accumulative number of completed SIP subscription attempts.
SIP_SUB_COUNT_STABLE	COUNTER	No	Indicates the current number of stable SIP subscription.
SIP_SUB_COUNT_TOTAL	COUNTER	No	Indicates the total number of current SIP subscription on this card (SIP_SUB_COUNT_ATTEMPTS + SIP_SUB_COUNT_CUM_COMPLETIONS).
RX_BYTES	COUNTER64	No	The number of received bytes.
TX_BYTES	COUNTER64	No	The number of transmitted bytes.
SIP_SUB_COUNT_FAILURE	COUNTER	False	Indicates the number of SIP relayed subscription failures.
CE_NAME	STRING	No	The name of the compute element for this entity.

SipTrunkGroupOptionsIntervalStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
ACNAME	STRING	Yes	The name of the address context.	False	N/A	No
ZNAME	STRING	Yes	The name of this zone.	False	N/A	No
SIP_TG_OPTIONS_NAME	STRING	Yes	The name of this SIP trunk group.	False	N/A	No

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
SIP_TG_OPTIONS_DIRECTION	STRING	Yes	The direction of the (interval) SIP Options/Response messages.	False	N/A	No
SIP_TG_OPTIONS_MESSAGE	STRING	Yes	The cause code of the (interval) SIP Options/Response messages.	False	N/A	No
SIP_TG_OPTIONS_MESSAGE_COUNT	COUNTER	No	The total number of (interval) SIP Options/Response messages for the specified cause code.	True	SUM	No
CE_NAME	STRING	No	The name of the compute element for this entity.	False	N/A	No

Sys Stats

SysCpuUtilIntStatsSts

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	This object indicates the configured CE name.	Show Status System
CPU	GAUGE	Yes	The CPU number.	
AVERAGE	GAUGE	No	The average CPU utilization for this interval.	
HIGH	GAUGE	No	The high CPU utilization for this interval.	
LOW	GAUGE	No	The low CPU utilization for this interval.	

SysMemoryUtilIntStatsSts

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	This object indicates the configured CE name.	Show Status System
AVERAGE	GAUGE	No	The average memory utilization for this interval.	
HIGH	GAUGE	No	The high memory utilization for this interval.	
LOW	GAUGE	No	The low memory utilization for this interval.	
AVERAGE_SWAP	GAUGE	No	The average swap memory utilization for this interval.	
HIGH_SWAP	GAUGE	No	The high swap memory utilization for this interval.	
LOW_SWAP	GAUGE	No	The low swap memory utilization for this interval.	

SystemCongestionIntervalStats

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
NAME	INTEGER	Yes	Name of the system.	False	Show Status System
LEVEL_MC1_COUNT	COUNTER	No	The number of transitions into MC1 for the specified interval.	False	
LEVEL_MC1_TOTAL_TIME	COUNTER	No	The sum of time spent in MC1 for the specified interval.	False	
LEVEL_MC2_COUNT	COUNTER	No	The number of transitions into MC2 for the specified interval.	False	
LEVEL_MC2_TOTAL_TIME	COUNTER	No	The sum of time spent in MC2 for the specified interval.	False	
LEVEL_MC3_COUNT	COUNTER	No	The number of transitions into MC3 for the specified interval.	False	
LEVEL_MC3_TOTAL_TIME	COUNTER	No	The sum of time spent in MC3 for the specified interval.	False	
OVERLOAD_REJECTS	COUNTER	No	The number of calls rejected due to System congestion for the specified interval.	False	
AVG_CALL_RATE	GAUGE	No	The system average call arrival rate for the specified interval.	False	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
PEAK_CALL_RATE	GAUGE	No	The system peak call arrival rate for the specified interval.	False	
CALL_ARRIVALS	COUNTER	No	The number of call arrivals for the specified interval.	False	
EMERGENCY_CALL_ARRIVALS	COUNTER	No	The number of SIP emergency calls arrived for the specified interval.	False	
EMERGENCY_CALL_REJECTS	COUNTER	No	The number of SIP emergency calls arrived for the specified interval.	False	
SIP_REG_ARRIVALS	COUNTER	No	The number of SIP registrations arrived for the specified interval.	False	
SIP_REG_REJECTS	COUNTER	No	The number of SIP registrations rejected for the specified interval.	False	
AVG_REG_RATE	GAUGE	No	The average SIP registration arrival rate for the specified interval.	False	
PEAK_REG_RATE	GAUGE	No	The peak SIP registration arrival rate for the specified interval.	False	
MAX_ACTIVE_CALLS	GAUGE	No	High watermark of the total number of active calls in current interval for system level.	True	

Column Name	Column Type	Index	Description	Aggregated	CLI Command Reference
SIP_SUBS_ARRIVALS	GAUGE	No	The current number of SIP subscribes arrived.	True	
SIP_SUBS_REJECTS	GAUGE	No	The current number of SIP subscribes rejected.	True	
AVG_SUBS_RATE	GAUGE	No	The current average SIP subscribe arrival rate.	True	
PEAK_SUBS_RATE	GAUGE	No	The current peak SIP subscribe arrival rate.	True	
CE_NAME	STRING	No	The name of the compute element for this entity.	False	

SystemLicenseInfoStats

Column Name	Column Type	Index	Description	CLI Command Reference
FEATURE_NAME	STRING	Yes	This object indicates the feature name	Show Table System
LICENSE_ID	STRING	Yes	This object indicates the license Id.	
EXPIRATION_DATE	STRING	No	This object indicates the licence expiry date for a feature.	
USAGE_LIMIT	INTEGER	No	This object indicates the usageLimit of a feature.	
SOURCE	STRING	No	This object indicates where the licenses is located, nodeLocked or domain.	

Column Name	Column Type	Index	Description	CLI Command Reference
IN_USE	GAUGE	No	This object indicates the number of licenses used by the application.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

SystemLicenseInfoStats is available only if SBC 3.1 Device Manager is installed.

TcpGeneralGroupStats

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	The name of the compute element for this entry.	NA
ESTABLISHED_CONNECTIONS	GAUGE	No	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT (currEstab).	
CLIENT_CONNECTIONS	COUNTER	No	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state (activeOpens).	
SERVER_CONNECTIONS	COUNTER	No	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state (passiveOpens).	

Column Name	Column Type	Index	Description	CLI Command Reference
FAILED_ATTEMPTS	COUNTER	No	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state (attemptFails).	
IN_SEGMENTS	COUNTER	No	The total number of segments received, including those received in error. This count includes segments received on currently established connections.	
OUT_SEGMENTS	COUNTER	No	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.	
RETRANS_SEGMENTS	COUNTER	No	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.	
IN_ERRORS	COUNTER	No	The total number of segments received in error (for example, bad TCP checksums).	
IN_RESETS	COUNTER	No	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state (estabResets).	

Column Name	Column Type	Index	Description	CLI Command Reference
OUT_RESETS	COUNTER	No	The number of TCP segments sent containing the RST flag.	

TrafficControlStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context zone.	
NAME	STRING	Yes	The name of this trunk group.	
SILC	GAUGE	No	The number of calls cancelled due to SILC for this trunk group for the specified interval.	
STR_CANT	GAUGE	No	The number of calls cancelled due to STR for this trunk group for the specified interval.	
STR_SKIP	GAUGE	No	The number of calls skipped due to STR for this trunk group for the specified interval.	
SKIP	GAUGE	No	The number calls skipped due to the SKIP traffic control for this trunk group for the specified interval.	
CANT	GAUGE	No	The number of calls cancelled due to CANT for this trunk group for the specified interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
CANF	GAUGE	No	The number of calls cancelled due to CANF for this trunk group for the specified interval.	
ACC_CANT	GAUGE	No	The number of calls cancelled due to ACC for this trunk group for the specified interval.	
ACC_SKIP	GAUGE	No	The number of calls skipped due to ACC for this trunk group for the specified interval.	
ROUTE_ATTEMPTS_IRR	GAUGE	No	The number of reroute attempts due to IRR for this trunk group for the specified interval.	
ROUTE_ATTEMPTS_SIRR	GAUGE	No	The number of reroute attempts due to SIRR for this trunk group for the specified interval.	
ROUTE_ATTEMPTS_ORR	GAUGE	No	The number of reroute attempts due to ORR for this trunk group for the specified interval.	
ROUTE_ATTEMPTS_SORR	GAUGE	No	The number of reroute attempts due to SORR for this trunk group for the specified interval.	
SUCCESSFUL_IRR	GAUGE	No	The number of successful reroutes due to IRR for this trunk group for the specified interval.	
SUCCESSFUL_SIRR	GAUGE	No	The number of successful reroutes due to SIRR for this trunk group for the specified interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
SUCCESSFUL_ORR	GAUGE	No	The number of successful reroutes due to ORR for this trunk group for the specified interval.	
SUCCESSFUL_SORR	GAUGE	No	The number of successful reroutes due to SORR for this trunk group for the specified interval.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

CURRENT_CLIENT_SESSIONS, CURRENT_SUSPENDED_SESSIONS, TOTAL_CLIENT_SESSIONS are not valid for SBC 4.0 and higher versions.

UdpGeneralGroupStats

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	Yes	The name of the compute element for this entry.	NA
IN_DATAGRAMS	COUNTER	No	The total number of UDP datagrams delivered to UDP users.	
OUT_DATAGRAMS	COUNTER	No	The total number of UDP datagrams sent from this entity.	
UNKNOWN_PORTS	COUNTER	No	The total number of received UDP datagrams for which there was no application at the destination port.	
IN_ERRORS	COUNTER	No	The number of received UDP datagrams that this entity cannot deliver for reasons other than the lack of an application at the destination port.	

ZoneIntervalStatisticsStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
NAME	STRING	Yes	The name of this zone.	
INGRESS_FAIL_CALL_LIMIT	COUNTER	No	Number of incoming Calls failed due to Call Limit check on Zone.	
EGRESS_FAIL_CALL_LIMIT	COUNTER	No	Number of outgoing Calls failed due to Call Limit check on Zone.	
INGRESS_FAIL_CALL_POLICIN G	COUNTER	No	Number of incoming Calls failed due to Call Policer check on Zone.	
EGRESS_FAIL_CALL_POLICIN G	COUNTER	No	Number of outgoing Calls failed due to Call Policer check on Zone.	
INGRESS_FAIL_BWLIMIT	COUNTER	No	Number of incoming Calls failed due to Bandwidth Limit check on Zone.	
EGRESS_FAIL_BWLIMIT	COUNTER	No	Number of outgoing Calls failed due to BW Limit check on Zone.	
INGRESS_SIP_REG_FAIL_LIMI T	COUNTER	No	Number of incoming SIP Registrations failed due to Registrations Limit check on Zone.	
EGRESS_SIP_R EG_FAIL_LIMIT	COUNTER	No	Number of outgoing SIP Registrations failed due to Registrations Limit check on Zone.	
INGRESS_SIP_REG_POLICING	COUNTER	No	Number of incoming SIP Registrations failed due to ingress Policer check on Zone.	

Column Name	Column Type	Index	Description	CLI Command Reference
EGRESS_SIP_R EG_POLICING	COUNTER	No	Number of outgoing SIP Registrations failed due to egress Policer check on Zone.	
VIDEO_THRES HOLD_LIMIT	COUNTER	No	The number of exceeded video threshold limits for this zone.	
CE_NAME	STRING	No	The name of the compute element for this entity.	

SBC CNF Statistics

In this section:

- [CallCountIntervalStats](#)
- [CallCountIntervalStats_AG](#)
- [CallFailIntervalStats](#)
- [CallFailIntervalStats_AG](#)
- [CallIntervalStats](#)
- [CallIntervalStats_AG](#)
- [CnfDnsGroupDnsServerStats](#)
- [CnfEthernetPortPacketStats](#)
- [CnflcmpGeneralGroupStats](#)
- [CnflpAcIOverallStats](#)
- [CnflpAcIOverallStats_AG](#)
- [CnflpAcIRuleStats](#)
- [CnflpAcIRuleStats_AG](#)
- [CnflpGeneralGroupStats](#)
- [CnflpPolicingSystemIntStats](#)
- [CnflpPolicingSystemIntStats_AG](#)
- [CnfLinkDetectionGroupStats](#)
- [CnfLinkMonitorStats](#)
- [CnfSBX5KAcIOffListIntStats](#)
- [CnfSBX5KAggregateOffIntStats](#)
- [CnfSBX5KArpOffListIntStats](#)
- [CnfSBX5KBadEtherIpHdrOffIntStats](#)
- [CnfSBX5KDiscardRuleOffIntStats](#)
- [CnfSBX5KEthernetPortPacketPortStatus](#)
- [CnfSBX5KIpSecDecryptOffIntStats](#)
- [CnfSBX5KMediaOffIntStats](#)
- [CnfSBX5KRogueMediaIntStats](#)
- [CnfSBX5KSipIpPeerIntervalStats](#)
- [CnfSBX5KSipOptResponseIntervalStats](#)
- [CnfSBX5KSrtpDecryptOffIntStat](#)

- CnfSBX5KUflowOffListIntStats
- CnfsipOcsCallIntervalStatistics
- CnfSibIntervalStatistics
- CnfSysCpuUtilIntStatsSts
- CnfSysMemoryUtilIntStatsSts
- CnfSystemCongestionIntervalStats
- CnfSystemCongestionIntervalStats_AG
- CnfTcpGeneralGroupStats
- CnfUdpGeneralGroupStats
- DspResDspCallIntervalStats
- DspResDspCallIntervalStats_AG
- DspResDspUsageIntervalStats
- DspResDspUsageIntervalStats_AG
- EthernetPortMgmtStats
- NBS5200CallCountStats
- NBS5200CallCountStats_AG
- NBS5200TGStatusStats_AG
- NBS5200TrunkGroupStatusStats
- SBCCOREOodMessageIntStats
- SBCCORESipRegCountDomIntStats
- SBCCORESipRegCountDomIntStats_AG
- SBCCORESipTgCSSRIntStats
- SBCCORESipTgCSSRIntStats_AG
- SBCCORESipTGResIntStats
- SBCCORESipTGResIntStats_AG
- SBX5KSipByeResponseIntervalStats
- SBX5KSipInviteResponseIntervalStats
- SBX5KSipRegResponseIntervalStats
- SBX5KSystemDspStatusDspUsageStats
- SipIntervalStats
- SipIntervalStats_AG
- SipIpPeerOptionsIntervalStats
- SipIpPeerOptionsIntervalStats_AG
- SipRegCountStats
- SipRegCountStats_AG
- SipSigConnStatisticsStats
- SipSigPortStatisticsStats
- SipSigPortStatisticsStats_AG
- SipSigPortTlsStats
- SipSubCountStats
- SipSubCountStats_AG
- SipTrunkGroupOptionsIntervalStats
- SipTrunkGroupOptionsIntervalStats_AG
- SystemLicenseInfoStats
- TrafficControlStats
- ZoneIntervalStatisticsStats
- ZoneIntervalStatisticsStats_AG

CallCountIntervalStats

Column Name	Column Type	Index	Description	canAggregate
NAME	INTEGER	True	This adds a dummy key to non-config scalar element container, even though only one row is allowed in container. Without the key, tailf treats the container non-dynamic and calls get_elem per leaf instead of calling get_object per row.	True
MAX_SESSION_COUNT	COUNTER	False	Displayed as maxSessionCallCount. The high watermark of total number of calls for the specified interval. This statistic accounts for calls that are stable.	True
MAX_POL_RTU_COUNT	INTEGER	False	Displays the same count as MAX_SESSION_COUNT if SBC is using SBC-POL-RTU license. If SBC is not using SBC-POL-RTU license, the count is displayed as 0.	True
ENCRYPT_COUNT	COUNTER	False	Displayed as system wide total encrypt Call Count. The high watermark of total number of encrypt calls for the specified interval.	True
SRTP_COUNT	COUNTER	False	Displayed as system wide total Secure Real-time Transport Protocol (SRTP) Call Count; The high watermark of total number of SRTP calls for the specified interval.	True
VIDEO_COUNT	COUNTER	False	Displayed as system wide total video Call Count; The high watermark of total number of video calls for the specified interval.	True
AMRNB_COUNT	COUNTER	False	The high watermark of total number of Adaptive Multi-Rate Narrowband (AMRNB) calls for the specified interval.	True
AMRWB_COUNT	COUNTER	False	The high watermark of total number of Adaptive Multi-Rate Wideband (AMRWB) calls for the specified interval.	True

Column Name	Column Type	Index	Description	canAggregate
EVRC_COUNT	COUNTER	False	The high watermark of total number of Enhanced Variable Rate Codec (EVRC) calls for the specified interval.	True
NICEREC_COUNT	COUNTER	False	The current high watermark of total number of NICE recording calls.	True
MRFSESS_COUNT	COUNTER	False	The current high watermark of total number of Media Resource Function (MRF) calls.	True
MAX_PSX_RTU_COUNT	INTEGER	False	Displays MAX_SESSION_COUNT when SBC is using SBC-PSX-RTU license. If SBC is not using SBC-PSX-RTU license it displays the count as 0.	True
VDSPRTU_COUNT	COUNTER	False	The high watermark of total number of trans-coded sessions for the specified interval.	True
PDCS_COUNT	COUNTER	False	The high watermark of total number of pdcs header sessions for the specified interval.	True
SIPREC_COUNT	COUNTER	False	The current high watermark of total number of sip recording calls.	True
LI_ENABLED	INTEGER	False	Set based on whether LI license is available at the SBC.	True
DSPG722_ENABLED	INTEGER	False	Set based on whether DspG722 license is available at the SBC.	True
GMP4X1_ENABLED	INTEGER	False	Set based on whether 4X1GMP license is available at the SBC.	True
SIPI_ENABLED	INTEGER	False	Set based on whether Sipl license is available at the SBC.	True
SIP323_ENABLED	INTEGER	False	Set based on whether SipRec license is available at the SBC.	True
GMP1X10_ENABLED	INTEGER	False	Set based on whether 1X10GMP license is available at the SBC.	True

Column Name	Column Type	Index	Description	canAggregate
CAPACITY_ENABLED	INTEGER	False	Set based on whether Capacity license is available at the SBC.	True
E911_ENABLED	INTEGER	False	Set based on whether E911 license is available at the SBC.	True
ENUM_ENABLED	INTEGER	False	Set based on whether ENUM license is available at the SBC.	True
SWINSTANCE_ENABLED	INTEGER	False	Set based on whether Swe Instance license is available at the SBC.	True
EVS_COUNT	COUNT	False	The high watermark of total number of Enhanced Voice Services (EVS) calls for the specified interval.	True
SILK_COUNT	COUNT	False	The high watermark of total number of SILK Codec Transcode calls for the specified interval.	True
SBCRCS_COUNT	COUNT	False	The high watermark of total number of OOD calls that use an RCS based service for the specified interval.	True
HPC_QUEUE_ATTEMPT	COUNT	False	The number of HPC calls successfully placed on HPC Call Queuing queues for the reporting interval.	True
SLBSESS_COUNT	COUNT	False	Displayed as system wide total stable SLB sessions Count. The high watermark of the total number of active calls for the reporting interval.	True
LBINSTANCE_ENABLED	INTEGER	False	Set based on whether SLB license is available at the SLB.	False
HPC_QUEUE_OVERFLOW	COUNT	False	The number of HPC calls which experienced unsuccessful call queuing attempts due to full queues for the reporting interval.	True
HPC_QUEUE_ABANDON	COUNT	False	The number of queued HPC calls abandoned before call completion during the reporting interval.	True

Column Name	Column Type	Index	Description	canAggregate
HPC_QUE_TIMEO UTS	COUNT	False	The number of HPC calls removed from the queue due to expiration of the queue timeout timer for the reporting interval.	True
HPC_CTL_TFC_E XEM	COUNT	False	The HPC traffic control exemptions for this reporting interval.	True
SOSBC_RTU_CO UNT	COUNTER	False	The system wide total stable SOSBC sessions count. The high water mark of total number of active calls for the reporting interval.	True
WEB_SOCKET_C OUNT	COUNTER	False	The high water mark of total number of web socket calls for this reporting interval.	True
NOTRUF_AUTH	INTEGER	True	Set based on whether NOTRUF license is available at the SBC.	False
CE_NAME	STRING	False	The name of the compute element for this entry.	False
CALL_COUNT_CN E	COUNTER	False	Displayed as system wide total CNE sessions Count. The high water mark of total number of active calls for the reporting interval.	True
L16_LEG_COUNT	COUNTER	False	The high water mark of total number of L16 call legs for the reporting interval.	True
T140	INTEGER	False	Set based on whether the t140 code is used on at least one call leg for the current interval.	True
DOD	INTEGER	False	Set based on when the application is running in DOD mode.	True
FIPS	INTEGER	False	Set based on when the application is running in FIPS mode.	True
CNEINSTANCE_E NABLED	INTEGER	False	Set based on whether cneInstance license is available at the SBC.	True

CallCountIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
NAME	INTEGER	True	This adds a dummy key to non-config scalar element container, even though only one row is allowed in container. Without the key, tailf treats the container non-dynamic and calls get_elem per leaf instead of calling get_object per row.	false	N/A
SUM_MAX_SESSION_COUNT	COUNTER	False	The sum of the high watermark of total number of calls for the specified interval. This statistic accounts for calls that are stable. Displayed as maxSessionCallCount.	True	SUM
SUM_MAX_POL_RTU_COUNT	INTEGER	False	The sum of the MAX_SESSION_COUNT if SBC is using SBC-POL-RTU license. If SBC is not using SBC-POL-RTU license, the count is displayed as 0.	True	SUM
SUM_ENCRYPT_COUNT	COUNTER	False	The sum of the system wide total encrypt Call Count. The high watermark of total number of encrypt calls for the specified interval.	True	
SUM_SRTP_COUNT	COUNTER	False	The sum of the system wide total Secure Real-time Transport Protocol (SRTP) Call Count; The high watermark of total number of SRTP calls for the specified interval.	True	SUM
SUM_VIDEO_COUNT	COUNTER	False	The sum of the system wide total video Call Count; The high watermark of total number of video calls for the specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_AMRNB_COUNT	COUNTER	False	The sum of the high watermark of total number of Adaptive Multi-Rate Narrowband (AMRNB) calls for the specified interval.	True	SUM
SUM_AMRWB_COUNT	COUNTER	False	The sum of the high watermark of total number of Adaptive Multi-Rate Wideband (AMRWB) calls for the specified interval.	True	SUM
SUM_EVRC_COUNT	COUNTER	False	The sum of the high watermark of total number of Enhanced Variable Rate Codec (EVRC) calls for the specified interval.	True	SUM
SUM_NICEREC_COUNT	COUNTER	False	The sum of the current high watermark of total number of NICE recording calls.	True	SUM
SUM_MRFSESS_COUNT	COUNTER	False	The sum of the current high watermark of total number of Media Resource Function (MRF) calls.	True	SUM
SUM_MAX_PSEX_RTU_COUNT	INTEGER	False	The sum of the MAX_SESSION_COUNT when SBC is using SBC-PSX-RTU license. If SBC is not using SBC-PSX-RTU license it displays the count as 0.	True	SUM
SUM_VDSPRTU_COUNT	COUNTER	False	The sum of the high watermark of total number of trans-coded sessions for the specified interval.	True	SUM
SUM_PDCS_COUNT	COUNTER	False	The sum of the high watermark of total number of pdcs header sessions for the specified interval.	True	SUM
SUM_SIPREC_COUNT	COUNTER	False	The sum of the current high watermark of total number of sip recording calls.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_LI_ENABLED	INTEGER	False	The sum of the count of LI licenses available at the SBC.	True	SUM
SUM_DSPG722_ENABLED	INTEGER	False	The sum of the count of DspG722 licenses available at the SBC.	True	SUM
SUM_GMP4X1_ENABLED	INTEGER	False	The sum of the count of 4X1GMP licenses is available at the SBC.	True	SUM
SUM_SIPI_ENABLED	INTEGER	False	The sum of the count of Sipl licenses available at the SBC.	True	SUM
SUM_SIP323_ENABLED	INTEGER	False	The sum of the count of SipRec licenses available at the SBC.	True	SUM
SUM_GMP1X10_ENABLED	INTEGER	False	The sum of the count of 1X10GMP licenses available at the SBC.	True	SUM
SUM_CAPACITY_ENABLED	INTEGER	False	The sum of the count of Capacity licenses available at the SBC.	True	SUM
SUM_E911_ENABLED	INTEGER	False	The sum of the count of E911 licenses available at the SBC.	True	SUM
SUM_ENUM_ENABLED	INTEGER	False	The sum of the count of ENUM licenses available at the SBC.	True	SUM
SUM_SWINSTANCE_ENABLED	INTEGER	False	The sum of the count of SWe Instance licenses available at the SBC.	True	SUM
SUM_EVS_COUNT	COUNT	False	The sum of the high watermark of total number of Enhanced Voice Services (EVS) calls for the specified interval.	True	SUM
SUM_SILK_COUNT	COUNT	False	The sum of the high watermark of total number of SILK Codec Transcode calls for the specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SBCRCS_COUNT	COUNT	False	The sum of the high watermark of total number of OOD calls that use an RCS based service for the specified interval.	True	SUM
SUM_LBINSTANCE_ENABLED	INTEGER	False	The sum of the count of SLB licenses available at the SLB.	True	SUM
SUM_SLB_SESSIONS_COUNT	COUNTER	False	The sum of the total stable SLB sessions count across the system. The high watermark of total number of active calls for the reporting interval.	True	SUM
SUM_HPC_QUEUE_ATTEMPT	COUNTER	False	The sum of the number of HPC calls that were successfully placed on HPC Call Queuing queues for the reporting interval.	True	SUM
SUM_HPC_QUEUE_OVERFLOW	COUNTER	False	The sum of the number of HPC calls for which HPC call queuing attempts were unsuccessful because queues were full for the reporting interval.	True	SUM
SUM_HPC_QUEUE_ABANDON	COUNTER	False	The sum of the number of HPC calls that were placed in HPC Call Queuing queues, but were subsequently abandoned before they are completed for the reporting interval.	True	SUM
SUM_HPC_QUEUE_TIMEOUTS	COUNTER	False	The sum of the number of HPC calls that were placed in HPC Call Queuing queues, but were subsequently abandoned before they are completed for the reporting interval.	True	SUM
SUM_HPC_CTL_TFC_EXEM	COUNTER	False	The sum of the HPC traffic control exemptions for this reporting interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SOSBC_RTU_COUNT	COUNTER	False	The system wide total stable SOSBC sessions count. The high water mark of total number of active calls for the reporting interval.	True	SUM
AVG_LBINSTANCE_ENABLED	INTEGER	False	Set based on whether the SLB license is available at the SLB.	True	MEAN
AVG_LICENSE_MODE	INTEGER	False	Displays the licensing mode of the SBC.	True	MEAN
WEB_SOCKET_COUNT	COUNTER	False	The high water mark of total number of web socket calls for this reporting interval.	True	SUM
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

CallFailIntervalStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context zone.	False	
NAME	STRING	Yes	The name of this trunk group.	True	
IN_CALL_FAIL_NO_ROUTES	COUNTER	No	Number of inbound failed calls because there was no route available for this trunk group for the specified interval.	False	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
IN_CALL_FAIL_NO_RESOURCES	COUNTER	No	Number of inbound failed calls because there was an unavailable resource for this trunk group for the specified interval.	True	
IN_CALL_FAIL_NO_SERVICE	COUNTER	No	Number of inbound failed calls because there was an unavailable service for this trunk group for the specified interval.	True	
IN_CALL_FAIL_INVALID_CALL	COUNTER	No	Number of inbound failed calls because there was an invalid call attempt for this trunk group for the specified interval.	True	
IN_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	Number of inbound failed calls because there was a network failure for this trunk group for the specified interval.	True	
IN_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	The number of failed inbound calls due to a protocol error for this trunk group for the specified interval. The SBC increments the counter for this statistic when it receives unrecognized parameters, or all the required parameters are not configured.	True	
IN_CALL_FAIL_UNSPECIFIED	COUNTER	No	Number of inbound failed calls for an unspecified reason for this trunk group for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
OUT_CALL_FAIL_NO_ROUTES	COUNTER	No	Number of outbound failed calls due to no route available for this trunk group for the specified interval.	True	
OUT_CALL_FAIL_NO_RESOURCES	COUNTER	No	The number of failed outbound calls due to unavailable resources for this trunk group for the specified interval. The SBC increments the counter for this statistic when the route is not configured and it fails to find the necessary resources.	True	
OUT_CALL_FAIL_NO_SERVICE	COUNTER	No	The number of failed outbound calls due to service unavailability for this trunk group for the specified interval. The SBC increments the counter for this statistic when outbound call service is not available for this trunk group during the specified interval.	True	
OUT_CALL_FAIL_INVALID_CALL	COUNTER	No	Number of outbound failed calls due to invalid call attempt for this trunk group for the specified interval.	True	
OUT_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	Number of outbound failed calls due to network failure for this trunk group for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
OUT_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	The number of failed outbound calls due to a protocol error for this trunk group for the specified interval. The SBC increments the counter for this statistic when it receives unrecognized parameters, or all the required parameters are not configured.	True	
OUT_CALL_FAIL_UNSPECIFIED	COUNTER	No	The number of failed outbound calls due to an unspecified reason for this trunk group for the specified interval. The SBC increments the counter for this statistic if the SIP Signaling Port for the egress is disabled while calls are in progress.	True	
ROUTING_FAILURES_RESERVED	COUNTER	No	Number of routing failures due to all circuits reserved for this trunk group for specified interval.	True	
ALLOC_FAIL_BW_LIMIT	COUNTER	No	The number of failed bandwidth requests due to the current usage exceeding the configured bandwidth limit for this trunk group for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ALLOC_FAIL_CALL_LIMIT	COUNTER	No	The number of failed call handling requests due to the current number of concurrent calls exceeding the configured call limit for this trunk group for the specified interval.	True	
NO_PSX_ROUTE	COUNTER	No	Number of failed calls on an ingress trunk group due to no routes returned from the ERE for the specified interval.	True	
CALL_ABANDONED	COUNTER	No	Number of calls on a toll-free TG that were abandoned while dialing for the specified interval.	True	
CALL_FAIL_POLICING	COUNTER	No	The number of calls for a trunk group that failed during the specified interval due to configured policing rules in the SBC.	True	
SIP_REG_FAIL_POLICING	COUNTER	No	Number SIP registration attempts that failed due to policing on TG for specified interval.	True	
SIP_REG_FAIL_INTERNAL	COUNTER	No	Number SIP registration attempts that failed due to other reasons (signaling failures, and so on) on a trunk group for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SIP_REG_FAIL_OTHER	COUNTER	No	The current number SIP registration attempts that failed due to other reasons (signaling failures, and so on) on a trunk group for the specified interval.	True	
SECURITY_FAIL	COUNTER	No	Number of calls that failed due to mismatch between the peer security and route packet service profile security on trunk group for specified interval.	True	
NON_REG_CALLS_FAILED	COUNTER	No	Number of failed calls due to registration requirement for SIP trunk group for the specified interval.	True	
NON_MATCH_SRC_IP_CALLS_FAIL	COUNTER	No	Number of calls that failed due to mismatched source IP of IAD according to its RCB for the specified interval.	True	
INVALID_SP_CALLS_FAILED	COUNTER	No	Number of failed calls due to mismatched ingress signaling port from CP according to RCB for the specified interval.	True	
SIP_SUBS_FAIL_POLICING	COUNTER	No	Number of SIP Subscribe attempts that failed due to policing on a trunk group.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SIP_OTHER_REQ_FAIL_POLICING	COUNTER	No	Number of SIP other non-invite attempts that failed due to policing on trunk group.	True	
SIP_OTHER_REQ_FAIL_INTERNAL	COUNTER	No	The count of SIP other non-invite attempts that failed due to policing on a trunk group.	True	
SIP_OTHER_REQ_FAIL_OTHER	COUNTER	No	The count of SIP other non-invite attempts that failed due to policing on a trunk group.	True	
VIDEO_THRESHOLD_LIMIT	COUNTER	No	The count of exceeded video threshold limits for this shared CAC limits pool.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

CallFailIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
ZNAME	STRING	Yes	The name of the address context zone.	False	N/A
NAME	STRING	Yes	The name of this trunk group.	False	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_IN_CALL_F AIL_NO_ROUTES	COUNTER	No	The sum of the number of inbound failed calls because there was no route available for this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_F AIL_NO_RESOURCE	COUNTER	No	The sum of the number of inbound failed calls because there was an unavailable resource for this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_F AIL_NO_SERVICE	COUNTER	No	The sum of the number of inbound failed calls because there was an unavailable service for this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_F AIL_INVALID_CALL	COUNTER	No	The sum of the number of inbound failed calls because there was an invalid call attempt for this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_F AIL_NETWORK_FAILURE	COUNTER	No	The sum of the number of inbound failed calls because there was a network failure for this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_F AIL_PROTOCOL_ERROR	COUNTER	No	The sum of the number of inbound failed calls because there was a protocol error for this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_F AIL_UNSPECIFIED	COUNTER	No	The sum of the number of inbound failed calls for an unspecified reason for this trunk group for the specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_OUT_CALL_FAIL_NO_ROUTE_S	COUNTER	No	The sum of the number of outbound failed calls due to no route available for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_NO_RESOURCES	COUNTER	No	The sum of the number of outbound failed calls due to unavailable resource for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_NO_SERVICE	COUNTER	No	The sum of the number of outbound failed calls due to unavailable service for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_INVALID_CALL	COUNTER	No	The sum of the number of outbound failed calls due to invalid call attempt for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_NETWORK_FAILURE	COUNTER	No	The sum of the number of outbound failed calls due to network failure for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_PROTOCOL_ERROR	COUNTER	No	The sum of the number of outbound failed calls due to protocol error for this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_FAIL_UNSPECIFIED	COUNTER	No	The sum of the number of outbound failed calls for an unspecified reason for this trunk group for the specified interval.	True	SUM
SUM_ROUTING_FAILURES_RESERVED	COUNTER	No	The sum of the number of routing failures due to all circuits reserved for this trunk group for specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_ALLOC_FAIL_BW_LIMIT	COUNTER	No	The sum of the number of bandwidth Requests which fail because the specified interval for this trunk group exceeds the configured bandwidth limit.	True	SUM
SUM_ALLOC_FAIL_CALL_LIMIT	COUNTER	No	The sum of the number of bandwidth Requests which fail because the specified interval for this trunk group exceeds the configured call limit.	True	SUM
SUM_NO_PBX_ROUTE	COUNTER	No	The sum of the number of failed calls on an ingress trunk group due to no routes returned from the ERE for the specified interval.	True	SUM
SUM_CALL_ABANDONED	COUNTER	No	The sum of the number of calls on a toll-free TG that were abandoned while dialing for the specified interval.	True	SUM
SUM_CALL_FAIL_POLICING	COUNTER	No	The sum of the number of calls on a trunk group that failed due to policing for the specified interval.	True	SUM
SUM_SIP_REG_FAIL_POLICING	COUNTER	No	The sum of the number SIP registration attempts that failed due to policing on TG for specified interval.	True	SUM
SUM_SIP_REG_FAIL_INTERNAL	COUNTER	No	The sum of the number SIP registration attempts that failed due to other reasons (signaling failures, and so on) on a trunk group for the specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SIP_REG_FAIL_OTHER	COUNTER	No	The sum of the current number SIP registration attempts that failed due to other reasons (signaling failures, and so on) on a trunk group for the specified interval.	True	SUM
SUM_SECURITY_FAIL	COUNTER	No	The sum of the number of calls that failed due to mismatch between the peer security and route packet service profile security on trunk group for specified interval.	True	SUM
SUM_NON_REG_CALLS_FAILED	COUNTER	No	The sum of the number of failed calls due to registration requirement for SIP trunk group for the specified interval.	True	SUM
SUM_NON_MATCH_SRC_IP_CALLS_FAIL	COUNTER	No	The sum of the number of calls that failed due to mismatched source IP of IAD according to its RCB for the specified interval.	True	SUM
SUM_INVALID_SP_CALLS_FAILED	COUNTER	No	The sum of the number of failed calls due to mismatched ingress signaling port from CP according to RCB for the specified interval.	True	SUM
SUM_SIP_SUBS_FAIL_POLICING	COUNTER	No	The sum of the number of SIP Subscribe attempts that failed due to policing on a trunk group.	True	SUM
SUM_SIP_OTHER_REQ_FAIL_POLICING	COUNTER	No	The sum of the number of SIP other non-invite attempts that failed due to policing on trunk group.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SIP_OTHER_REQ_FAIL_INTERNAL	COUNTER	No	The number of SIP other non-invite attempts that failed due to policing on a trunk group.	True	SUM
SUM_SIP_OTHER_REQ_FAIL_OTHER	COUNTER	No	The number of SIP other non-invite attempts that failed due to policing on a trunk group.	True	SUM
SUM_VIDEO_THRESHOLD_LIMIT	COUNTER	No	The number of video threshold limit exceeded for this trunk group for the specified interval.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

CallIntervalStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context zone.	False	
NAME	STRING	Yes	The name of this trunk group.	True	
IN_USAGE	COUNTER	No	The duration, in seconds, for which all inbound calls in a given interval are using the trunkgroup. This metric is derived using the formula: (total # of inbound calls on the TG) * (interval size) * 60	False	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
OUT_USAGE	COUNTER	No	The duration, in seconds, for which all outbound calls in a given interval are using the trunkgroup. This metric is derived using the formula: (total # of outbound calls on the TG) * (interval size) * 60.	True	
IN_CALLS	COUNTER	No	Number of completed inbound calls on this trunk group for the specified interval.	True	
OUT_CALLS	COUNTER	No	Number of completed outbound calls on this trunk group for the specified interval.	True	
IN_CALL_ATTEMPTS	COUNTER	No	Number of inbound call attempts on this trunk group for the specified interval.	True	
OUT_CALL_ATTEMPTS	COUNTER	No	Number of outbound call attempts on this trunk group for the specified interval.	True	
MAX_COMPLETED_CALLS	COUNTER	No	The high watermark of total number of active calls in both the inbound and outbound directions on the trunk group for the specified interval. This statistic accounts for calls that are setting up, stable, or tearing down.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
CALL_SETUP_TIME	COUNTER	No	Total call setup time for all completed calls in inbound and outbound directions for this trunk group for specified interval measured in hundredths of a second.	True	
CALL_SETUPS	COUNTER	No	Total number of calls setup but not necessarily completed in the inbound and outbound directions for this trunk group for the specified interval.	True	
ROUTING_ATTEMPTS	COUNTER	No	The number of routing attempts for this trunk group for the specified interval. Each PSX dip can return up to 200 routes. The SBC selects routes based on a number of criteria such as CAC and bandwidth availability. In some cases, crankback/ route advance is needed if the first selected route fails. This metric counts the number of routes attempted before the call succeeded. If the first route succeeds, this counter = 1.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
IN_BW_USAGE	COUNTER	No	Sum of bandwidth usage (expected data rate in Kbits per second multiplied by call duration in seconds) for every inbound call associated with this trunk group for the specified interval.	True	
OUT_BW_USAGE	COUNTER	No	Sum of bandwidth usage (expected data rate in Kbits per second multiplied by call duration in seconds) in the outbound direction for this trunk group in seconds in the current interval. The trunk group usage is defined as the time a trunk is seized to the time a trunk is released.	True	
MAX_ACTIVE_BW_USAGE	GAUGE	No	High watermark bandwidth usage (in Kbits per second) in either direction associated with this trunk group for the specified interval.	True	
CALLS_WITH_PKT_OUTAGE	COUNTER	No	Number of calls with a maximum packet outage whose duration exceeds the configured minimum for this trunk group for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
CALLS_WITH_PKT_OUTAGE_AT_END	COUNTER	No	Number of calls whose maximum packet outage occurs at the end of the call for this trunk group for the specified interval.	True	
TOTAL_PKT_OUTAGE	COUNTER	No	Summation of packet outage duration (in milliseconds) whose duration exceeds the configured minimum which is reported during the specified performance interval.	True	
MAX_PKT_OUTAGE	GAUGE	No	Single longest maximum reported packet outage duration (in milliseconds) experienced during the specified performance interval for this trunk group.	True	
POD_EVENTS	COUNTER	No	Number of Packet Outage Detection (POD) Events detected for this peer group for the specified interval.	True	
PLAYOUT_BUFFER_GOOD	COUNTER	No	Number of calls with all sub-intervals reporting GOOD playout buffer quality for this trunk group for the specified interval.	True	
PLAYOUT_BUFFER_ACCEPTABLE	COUNTER	No	Number of calls with all sub-intervals reporting ACCEPTABLE or better playout buffer quality for this trunk group for the specified interval.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
PLAYOUT_BUFFER_POOR	COUNTER	No	Number of calls with all sub-intervals reporting POOR or better playout buffer quality for this trunk group for the specified interval.	True	
PLAYOUT_BUFFER_UNACCEPTABLE	COUNTER	No	Number of calls with at least one sub-interval reporting UNACCEPTABLE playout buffer quality for this trunk group for the specified interval.	True	
SIP_REG_ATTEMPTS	COUNTER	No	Current number of SIP registration attempts on a trunk group for the specified interval.	True	
SIP_REG_COMPLETIONS	COUNTER	No	Current number of SIP registrations that have successfully completed on a trunk group for the specified interval.	True	
CALLS_WITH_PBX_DIPS	COUNTER	No	The number of calls that made a PBX Dip during the interval (applies to ERE, ePBX and external ePBX).	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
TOTAL_PSX_DIPS	COUNTER	No	The total number of PSX dips for the specified interval (applies to ERE, ePSX and external ePSX). To see the number of calls which made PSX Dips during the interval, see CALLS_WITH_PSX_DIPS metric. Example During the specified interval, two calls made three dips each (due to call redirection, etc.) to the PSX. This is logged as: CALLS_WITH_PSX_DIPS = 2 and TOTAL_PSX_DIPS = 6. If calls do not involve redirection or other complex scenarios such as two-stage dialing and transfers, these two metrics can use the same value.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACTIVE_REGS	COUNTER	No	Interval number of active registrations on this trunk group.	True	
MAX_ACTIVE_REGS	GAUGE	No	Maximum active registrations on this trunk group (high-watermark achieved on this trunk group).	True	
CALL_LIMIT	GAUGE	No	CALL_LIMIT is the summation of TOTAL_CALLS_AVAILABLE, INBOUND_CALLS_USAGE, PRIORITY_CALL_USAGE, and OUTBOUND_CALLS_USAGE from NBS5200TrunkGroup StatusStats table (when it is not unlimited). Note CALL_LIMIT is different from the Call Limit configured at the SBC 5x00 device.	True	
ACTIVE_SUBS	COUNTER	No	Current number of active subscriptions on this trunk group.	True	
MAX_ACTIVE_SUBS	GAUGE	No	Maximum number of active subscriptions on this trunk group (high-watermark achieved on this trunk group).	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
PEAK_CALL_RATE	GAUGE	No	The current system peak call arrival rate.	True	
ONGOING_CALLS	INTEGER	No	Total number of ongoing calls (nonstable + stable) on this trunk group	True	
STABLE_CALLS	INTEGER	No	Total number of stable calls on this trunk group	True	
CALL_UPDATES	INTEGER	No	Total number of call updates on this trunk group	True	
EMERGENCY_STABLE_CALLS	INTEGER	No	Total number of stable emergency calls on this trunk group	True	
EMERGENCY_ONGOING_CALLS	INTEGER	No	Total number of emergency calls (stable + nonstable) on this trunk group	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

CallIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
ZNAME	STRING	Yes	The name of the address context zone.	False	N/A
NAME	STRING	Yes	The name of this trunk group.	False	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_IN_USAGE	COUNTER	No	The duration, in seconds, for which all inbound calls in a given interval are using the trunkgroup. This metric is derived using the formula: (total # of inbound calls on the TG) * (interval size) * 60	True	SUM
SUM_OUT_USAGE	COUNTER	No	The duration, in seconds, for which all outbound calls in a given interval are using the trunkgroup. This metric is derived using the formula: (total # of outbound calls on the TG) * (interval size) * 60.	True	SUM
SUM_IN_CALLS	COUNTER	No	Number of completed inbound calls on this trunk group for the specified interval.	True	SUM
SUM_OUT_CALLS	COUNTER	No	Number of completed outbound calls on this trunk group for the specified interval.	True	SUM
SUM_IN_CALL_ATTEMPTS	COUNTER	No	Number of inbound call attempts on this trunk group for the specified interval.	True	SUM
SUM_OUT_CALL_ATTEMPTS	COUNTER	No	Number of outbound call attempts on this trunk group for the specified interval.	True	SUM
SUM_MAX_COMPLETED_CALLS	COUNTER	No	The maximum number of completed calls in the inbound and outbound direction for this peer group for the specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_CALL_SETUP_TIME	COUNTER	No	Total call setup time for all completed calls in inbound and outbound directions for this trunk group for specified interval measured in hundredths of a second.	True	SUM
SUM_CALL_SETUPS	COUNTER	No	Total number of calls setup but not necessarily completed in the inbound and outbound directions for this trunk group for the specified interval.	True	SUM
SUM_ROUTING_ATTEMPTS	COUNTER	No	The number of routing attempts for this trunk group for the specified interval. Each PSX dip can return up to 200 routes. The SBC selects routes based on a number of criteria such as CAC and bandwidth availability. In some cases, crankback/ route advance is needed if the first selected route fails. This metric counts the number of routes attempted before the call succeeded. If the first route succeeds, this counter = 1.	True	SUM
SUM_IN_BW_USAGE	COUNTER	No	Sum of bandwidth usage (expected data rate in bits per second multiplied by call duration in seconds) for every inbound call associated with this trunk group for the specified interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_OUT_BW_USAGE	COUNTER	No	Sum of bandwidth usage (expected data rate in bits per second multiplied by call duration in seconds) for every outbound call associated with this trunk group for the specified interval.	True	SUM
AVG_MAX_ACTIVE_BW_USAGE	GAUGE	No	The high water mark of BW usage in either direction associated with this peer group for the specified interval.	True	MEAN
SUM_CALLS_WITH_PKT_OUTAGE	COUNTER	No	Number of calls with a maximum packet outage whose duration exceeds the configured minimum for this trunk group for the specified interval.	True	SUM
SUM_CALLS_WITH_PKT_OUTAGE_AT_END	COUNTER	No	Number of calls whose maximum packet outage occurs at the end of the call for this trunk group for the specified interval.	True	SUM
SUM_TOTAL_PKT_OUTAGE	COUNTER	No	Summation of packet outage durations (in milliseconds) whose duration exceeds the configured minimum which is reported during the specified performance interval.	True	SUM
AVG_MAX_PKT_OUTAGE	GAUGE	No	The single longest maximum reported packet outage duration (in milliseconds) experienced during the specified performance interval for this peer group.	True	MEAN

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_POD_EVENTS	COUNTER	No	Number of Packet Outage Detection (POD) Events detected for this peer group for the specified interval.	True	SUM
SUM_PLAYOUT_BUFFER_GOOD	COUNTER	No	Number of calls with all sub-intervals reporting GOOD playout buffer quality for this trunk group for the specified interval.	True	SUM
SUM_PLAYOUT_BUFFER_ACCEPTABLE	COUNTER	No	Number of calls with all sub-intervals reporting ACCEPTABLE or better playout buffer quality for this trunk group for the specified interval.	True	SUM
SUM_PLAYOUT_BUFFER_POOR	COUNTER	No	Number of calls with all sub-intervals reporting POOR or better playout buffer quality for this trunk group for the specified interval.	True	SUM
SUM_PLAYOUT_BUFFER_UNACCEPTABLE	COUNTER	No	Number of calls with at least one sub-interval reporting UNACCEPTABLE playout buffer quality for this trunk group for the specified interval.	True	SUM
SUM_SIP_REG_ATTEMPTS	COUNTER	No	The current number of SIP registration attempts on a peer group for the specified interval.	True	SUM
SUM_SIP_REG_COMPLETIONS	COUNTER	No	The current number of SIP registrations that have successfully completed on a peer group for the specified interval.	True	SUM
SUM_CALLS_WITH_PSX_DIPS	COUNTER	No	The number of calls that made a PSX Dip during the interval (applies to ERE, ePSX and external ePSX).	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_TOTAL_PSX_DIPS	COUNTER	No	The total number of PSX dips for the specified interval (applies to ERE, ePSX and external ePSX). To see the number of calls which made PSX Dips during the interval, see CALLS_WITH_PSX_DIPS metric. Example During the specified interval, two calls made three dips each (due to call redirection, etc.) to the PSX. This is logged as: CALLS_WITH_PSX_DIPS = 2 and TOTAL_PSX_DIPS = 6. If calls do not involve redirection or other complex scenarios such as two-stage dialing and transfers, these two metrics can use the same value.	True	SUM
SUM_ACTIVE_REGS	COUNTER	No	The Interval number of active registrations on this peer group.	True	SUM
AVG_MAX_ACTIVE_REGS	GAUGE	No	The Interval number of maximum active registrations on this peer group (this is the high-watermark achieved on this peer group).	True	MEAN
SUM_ACTIVE_SUBS	COUNTER	No	The Interval number of active subscribe on this peer group.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_MAX_ACTIVE_SUBS	GAUGE	No	The Interval number of maximum active subscribe on this peer group (this is the high-watermark achieved on this peer group).	True	MEAN
AVG_PEAK_CALL_RATE	GAUGE	No	Peak call arrival rate within a specified interval on this trunk group.	True	MEAN
AVG_ONGOING_CALLS	INTEGER	No	Total On Going Calls (Non-Stable + Stable) on this trunk group.	True	MEAN
AVG_STABLE_CALLS	INTEGER	No	Total Stable Calls on this trunk group.	True	MEAN
AVG_CALL_UPDATES	INTEGER	No	Total Call Updates on this trunk group.	True	MEAN
AVG_EMERGENCY_STABLE_CALLS	INTEGER	No	Total Emergency Stable Calls on this trunk group.	True	MEAN
AVG_EMERGENCY_ONGOING_CALLS	INTEGER	No	Total Emergency Calls Stable + Non-Stable on this trunk group.	True	MEAN
AVG_CALL_LIMIT	GAUGE	No	The sum of TOTAL_CALLS_AVAILABLE, INBOUND_CALLS_USAGE, PRIORITY_CALL_USAGE, and OUTBOUND_CALLS_USAGE from NBS5200TrunkGroupStatusStats table.	True	MEAN
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

CnfDnsGroupDnsServerStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ACNAME	STRING	True	The name of the address context.	True	
CNF_PODNAME	STRING	True	The name of the pod.	False	
GNAME	STRING	True	The name of the address context group.	False	
IND	GAUGE	True	The DNS server statistics isIndex for this address context.	False	
IP_ADDRESS	INETADDRESS	False	The IP address of the requested DNS server requested for statistics data.	False	
QUERIES	GAUGE	False	The number of queries made by the DNSC client to this DNS server.	True	
TIMEOUTS	GAUGE	False	The number of timeouts resulting from the queries made by the DNSC client to this DNS server.	True	
ERRORS	GAUGE	False	The number of errors resulting from the queries made by the DNSC client to this DNS server.	True	
REFERRALS	GAUGE	False	The number of referrals resulting from the queries made by the DNSC client to this DNS server.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
TOTAL_TCP_CONNECTION	GAUGE	False	The number tries for connecting to the DNS server.	True	
TCP_CONNECTION_FAILED	GAUGE	False	Number of times the SBC failed to connect to the DNS server.	True	
TCP_CONNECTION_SUCCESS	GAUGE	False	The number of successful TCP connections to the DNS server.	True	
TCP_CONNECTION_TORN_DOWN	GAUGE	False	Number of TCP connections torn down with the DNS server.	True	
TCP_FALLBACK	GAUGE	False	Number of times the TCP fallback to the DNS server.	True	
EDNS_STATUS	INTEGER	False	Number of times the TCP fallback to the DNS server.	True	
EDNS_FAILURES	GAUGE	False	Number of times the TCP fallback to the DNS server.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfEthernetPortPacketStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	True	The host name of the server.	False	
PORT_NAME	STRING	True	The name of the port.	False	
RX_PACKETS	COUNTER	False	The number of packets received.	True	
TX_PACKETS	COUNTER	False	The number of packets transmitted.	True	
RX_ERRORS	COUNTER	False	The number of bad packets received.	True	
TX_ERRORS	COUNTER	False	The number of packet transmit failures.	True	
RX_DROPPED	COUNTER	False	The number of packets dropped due to no receive buffers.	True	
TX_DROPPED	COUNTER	False	The number of packets dropped due to no transmit buffers.	True	
RX_BYTES	COUNTER	False	The number of bytes received.	True	
TX_BYTES	COUNTER	False	The number of bytes transmitted.	True	

CnflcmpGeneralGroupStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	True	The name of the compute element for this entry.	False	
IN_MSGS	COUNTER	False	The total number of ICMP messages received by this entity. Note This counter includes messages counted by icmpInErrors.	True	
IN_ECHOS	COUNTER	False	The number of ICMP Echo (request) messages received.	True	
IN_ECHO_REPS	COUNTER	False	The number of ICMP Echo reply messages received.	True	
IN_DEST_UNREACHS	COUNTER	False	The number of ICMP Destination Unreachable messages received.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
IN_ERRORS	COUNTER	False	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).	True	
OUT_MSGS	COUNTER	False	The total number of ICMP messages attempted to send by this entity. Note This counter includes all messages counted by icmpOutErrors.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
OUT_ERRORS	COUNTER	False	The number of ICMP messages which this entity did not send due to problems discovered within the ICMP. For example, lack of buffer. This value should not include errors discovered outside the ICMP layer. For example, the inability of IP to route the resultant datagram. Based on the implementation, there may be no errors with respect to storageDataTypes, which contribute to this counter's value.	True	
OUT_ECHOS	COUNTER	False	The number of ICMP Echo (request) messages sent.	True	
OUT_ECHO_REPS	COUNTER	False	The number of ICMP Echo reply messages sent.	True	
OUT_DEST_UNREACHS	COUNTER	False	The number of ICMP destination unreachable messages sent.	True	

CnflpAcIOverallStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ACNAME	STRING	True	The name of the address context.	False	
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	True	The host name of the server.	False	
NAME	IMPLIEDSTRING	True	The name of the address context.	False	
MATCHED_NO_RULE	COUNTER	False	The number of times no rule has been matched.	True	

CnflpAcIOverallStats_AG

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ACNAME	STRING	True	The name of the address context.	False	
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	True	The host name of the server.	False	
NAME	IMPLIEDSTRING	True	The name of the address context.	False	
MATCHED_NO_RULE	COUNTER	False	The number of times no rule has been matched.	True	

CnflpAcIRuleStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ACNAME	STRING	True	The name of the address context.	False	
CNF_PODNAME	STRING	True	The name of the pod.	False	
NAME	STRING	True	The name of this IP access control list rule.	False	
MATCHES	COUNTER	False	The number of times this rule has been matched.	True	
POLICER_DISCARDS	COUNTER	False	The number of times the policer for this rule discarded packets.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnflpAcIRuleStats_AG

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ACNAME	STRING	True	The name of the address context.	False	
CNF_PODNAME	STRING	True	The name of the pod.	False	
NAME	STRING	True	The name of this IP access control list rule.	False	
MATCHES	COUNTER	False	The number of times this rule has been matched.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
POLICER_DISCARDS	COUNTER	False	The number of times the policer for this rule discarded packets.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnflpGeneralGroupStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	True	The name of the compute element for this entry.	False	
IN_RECEIVES	COUNTER	False	The total number of input datagrams received from interfaces, including those received in error.	True	
IN_HDR_ERRORS	COUNTER	False	The number of input datagrams discarded due to errors in IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
IN_ADDR_ERRORS	COUNTER	False	The number of input datagrams discarded due to invalid address in the IP address header destination. This count includes invalid addresses, for example, 0.0.0.0. It also includes addresses of unsupported classes, for example, 0.0.0.0. For entities which are not IP routers and do not forward datagrams, this counter includes discarded datagrams due to destination address not being a local address.	True	
IN_UNKNOWN_PROTOCOLS	COUNTER	False	The number of locally-addressed datagrams received successfully, but discarded because of an unknown or unsupported protocol.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
IN_DISCARDS	COUNTER	False	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded, for example, lack of buffer space. Note This counter does not include any datagrams discarded while awaiting re-assembly.	True	
IN_DELIVERS	COUNTER	False	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
OUT_REQUE STS	COUNTER	False	The total number of IP datagrams in which the local IP user- protocols (including ICMP) supplied to IP, in requests for transmission. Note This counter does not include any datagram s counted in ipForwDat agrams.		

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
OUT_DISCARDS	COUNTER	False	The number of output IP datagrams for which no problem was encountered to prevent their transmission to the destination, but which were discarded, for example, due to lack of buffer space. Note This counter includes datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
OUT_NO_ROUTES	COUNTER	False	The number of IP datagrams discarded because no route is found to transmit them to their destination. Note This counter includes any packets counted in ipForwDatagrams which meets the no-route criterion. Note This includes any datagram which a host cannot route because all of its default routers are down.	True	
REASM_TIME_OUT	INTEGER	False	The maximum number of seconds for which received fragments are held while awaiting reassembly at this entity.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
REASM_REQDS	COUNTER	False	The number of IP fragments received which needs to be reassembled at this entity.	True	
REASM_OKS	COUNTER	False	The number of IP datagrams successfully re-assembled.	True	
REASM_FAILURES	COUNTER	False	The number of failures detected by the IP re-assembly algorithm, for example, timed out, errors, etc). Note This is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
FRAG_OKS	COUNTER	False	The number of IP datagrams that have been successfully fragmented at this entity.	True	
FRAG_FAILS	COUNTER	False	The number of IP datagrams that are discarded because they need to be fragmented at this entity but could not be. For example, their Don't Fragment flag was set.	True	

CnflpPolicingSystemIntStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	False	The name of the compute element for this entry.	False	
SYSTEM_NAME	STRING	True	Name of the system.	False	
BAD_HDR_DISCARD_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the bad Ethernet/IP Header policer.	True	
BAD_HDR_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the bad Ethernet/IP Header policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
BAD_HDR_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the bad Ethernet/IP Header policer.	True	
BAD_HDR_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the bad Ethernet/IP Header policer.	True	
BAD_HDR_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the bad Ethernet/IP Header policer.	True	
BAD_HDR_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the bad Ethernet/IP Header policer.	True	
ARP_DISCARDED_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the ARP policer.	True	
ARP_ACCEPT_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the ARP policer.	True	
ARP_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the ARP policer.	True	
ARP_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the ARP policer.	True	
ARP_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the ARP policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ARP_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the ARP policer.	True	
ARP_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the ARP.	True	
UFLOW_DISCARD_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the micro flow policer.	True	
UFLOW_ACCEPT_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the micro flow policer.	True	
UFLOW_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the micro flow policer.	True	
UFLOW_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the micro flow policer.	True	
UFLOW_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the micro flow policer.	True	
UFLOW_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the micro flow policer.	True	
UFLOW_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the micro flow policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ACL_DISCARD_PACKET_COUNT	GAUGE	False	The current number of discarded packets for the access control list policer.	True	
ACL_ACCEPT_PACKET_COUNT	GAUGE	False	The current number of discarded packets for the access control list policer.	True	
ACL_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the access control list policer.	True	
ACL_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the access control list policer.	True	
ACL_MINOR_ALARM_DURATION	GAUGE	False	The current duration of minor alarms in seconds for the access control list policer.	True	
ACL_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the access control list policer.	True	
ACL_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the access control list policer.	True	
AGGREGATE_DISCARD_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the aggregate policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
AGGREGATE_ACCEPT_PACKET_COUNT	COUNTER	False	The current number of accepted packets for the aggregate policer.	True	
AGGREGATE_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the aggregate policer.	True	
AGGREGATE_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the aggregate policer.	True	
AGGREGATE_MINOR_ALARM_DUR	GAUGE	False	The current duration of the minor alarms in seconds for the aggregate policer.	True	
AGGREGATE_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the aggregate policer.	True	
AGGREGATE_MAJOR_ALARM_DUR	GAUGE	False	The current duration of the major alarms in seconds for the aggregate policer.	True	
IP_DISCARD_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the IPSEC Decrypt policer.	True	
IP_ACCEPT_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the IPSEC Decrypt policer.	True	
IP_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the IPSEC Decrypt policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
IP_MINOR_ALARM_COUNT	COUNTER	False	The current number of minor alarms for the IPSEC Decrypt policer.	True	
IP_MINOR_ALARM_DURATION	COUNTER	False	The current duration of the minor alarms in seconds for the IPSEC Decrypt policer.	True	
IP_MAJOR_ALARM_COUNT	COUNTER	False	The current number of major alarms for the IPSEC Decrypt policer.	True	
IP_MAJOR_ALARM_DURATION	COUNTER	False	The current duration of the major alarms in seconds for the IPSEC Decrypt policer.	True	
MEDIA_DISCARD_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the media policer.	True	
MEDIA_ACCEPT_PACKET_COUNT	COUNTER	False	The current number of accepted packets for the media policer.	True	
MEDIA_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the media policer.	True	
MEDIA_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the media policer.	True	
MEDIA_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the media policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
MEDIA_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the media policer.	True	
ROGUE_MEDIA_DISCARD_PKT_COUNT	COUNTER	False	The current number of discarded packets for the rogue media policer.	True	
ROGUE_MEDIA_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the rogue media policer.	True	
ROGUE_MEDIA_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the rogue media policer.	True	
ROGUE_MEDIA_MINOR_ALARM_DUR	GAUGE	False	The current duration of the minor alarms in seconds for the rogue media policer.	True	
ROGUE_MEDIA_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the rogue media policer.	True	
ROGUE_MEDIA_MAJOR_ALARM_DUR	GAUGE	False	The current duration of the major alarms in seconds for the rogue media policer.	True	
DISCARD_RULE_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the IPSEC Decrypt policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
DISCARD_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the discard rule.	True	
DISCARD_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the discard rule.	True	
DISCARD_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the discard rule.	True	
DISCARD_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the discard rule.	True	
DISCARD_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the discard rule.	True	
DECRYPT_DISCARD_PACKET_COUNT	COUNTER	False	The current number of packets discarded by SRTP decrypt discards.	True	
PEAK_DECRYPT_DISCARD_RATE	GAUGE	False	The current peak discard rate for SRTP decrypt discards.	True	
MINOR_DECRYPT_ALARM_COUNT	INTEGER	False	The current number of minor alarms for SRTP decrypt discards.	True	
MINOR_DECRYPT_ALARM_DURATION	INTEGER	False	The current duration of the minor alarms in seconds for SRTP decrypt discards.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
MAJOR_DECRYPT_ALARM_COUNT	INTEGER	False	The current number of major alarms for the SRTP decrypt discards.	True	
MAJOR_DECRYPT_ALARM_DURATION	INTEGER	False	The current duration of the major alarms in seconds for SRTP decrypt discards.	True	

CnflpPolicingSystemIntStats_AG

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	False	The name of the compute element for this entry.	False	
SYSTEM_NAME	STRING	True	Name of the system.	False	
BAD_HDR_DISCARD_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the bad Ethernet/IP Header policer.	True	
BAD_HDR_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the bad Ethernet/IP Header policer.	True	
BAD_HDR_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the bad Ethernet/IP Header policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
BAD_HDR_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the bad Ethernet/IP Header policer.	True	
BAD_HDR_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the bad Ethernet/IP Header policer.	True	
BAD_HDR_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the bad Ethernet/IP Header policer.	True	
ARP_DISCARDED_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the ARP policer.	True	
ARP_ACCEPT_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the ARP policer.	True	
ARP_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the ARP policer.	True	
ARP_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the ARP policer.	True	
ARP_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the ARP policer.	True	
ARP_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the ARP policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ARP_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the ARP.	True	
UFLOW_DISCARD_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the micro flow policer.	True	
UFLOW_ACCEPT_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the micro flow policer.	True	
UFLOW_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the micro flow policer.	True	
UFLOW_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the micro flow policer.	True	
UFLOW_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the micro flow policer.	True	
UFLOW_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the micro flow policer.	True	
UFLOW_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the micro flow policer.	True	
ACL_DISCARD_PACKET_COUNT	GAUGE	False	The current number of discarded packets for the access control list policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ACL_ACCEPT_PACKET_COUNT	GAUGE	False	The current number of discarded packets for the access control list policer.	True	
ACL_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the access control list policer.	True	
ACL_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the access control list policer.	True	
ACL_MINOR_ALARM_DURATION	GAUGE	False	The current duration of minor alarms in seconds for the access control list policer.	True	
ACL_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the access control list policer.	True	
ACL_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the access control list policer.	True	
AGGREGATE_DISCARD_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the aggregate policer.	True	
AGGREGATE_ACCEPT_PACKET_COUNT	COUNTER	False	The current number of accepted packets for the aggregate policer.	True	
AGGREGATE_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the aggregate policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
AGGREGATE_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the aggregate policer.	True	
AGGREGATE_MINOR_ALARM_DUR	GAUGE	False	The current duration of the minor alarms in seconds for the aggregate policer.	True	
AGGREGATE_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the aggregate policer.	True	
AGGREGATE_MAJOR_ALARM_DUR	GAUGE	False	The current duration of the major alarms in seconds for the aggregate policer.	True	
IP_DISCARD_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the IPSEC Decrypt policer.	True	
IP_ACCEPT_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the IPSEC Decrypt policer.	True	
IP_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the IPSEC Decrypt policer.	True	
IP_MINOR_ALARM_COUNT	COUNTER	False	The current number of minor alarms for the IPSEC Decrypt policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
IP_MINOR_ALARM_DURATION	COUNTER	False	The current duration of the minor alarms in seconds for the IPSEC Decrypt policer.	True	
IP_MAJOR_ALARM_COUNT	COUNTER	False	The current number of major alarms for the IPSEC Decrypt policer.	True	
IP_MAJOR_ALARM_DURATION	COUNTER	False	The current duration of the major alarms in seconds for the IPSEC Decrypt policer.	True	
MEDIA_DISCARD_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the media policer.	True	
MEDIA_ACCEPT_PACKET_COUNT	COUNTER	False	The current number of accepted packets for the media policer.	True	
MEDIA_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the media policer.	True	
MEDIA_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the media policer.	True	
MEDIA_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the media policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
MEDIA_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the media policer.	True	
ROGUE_MEDIA_DISCARD_PKT_COUNT	COUNTER	False	The current number of discarded packets for the rogue media policer.	True	
ROGUE_MEDIA_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the rogue media policer.	True	
ROGUE_MEDIA_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the rogue media policer.	True	
ROGUE_MEDIA_MINOR_ALARM_DUR	GAUGE	False	The current duration of the minor alarms in seconds for the rogue media policer.	True	
ROGUE_MEDIA_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the rogue media policer.	True	
ROGUE_MEDIA_MAJOR_ALARM_DUR	GAUGE	False	The current duration of the major alarms in seconds for the rogue media policer.	True	
DISCARD_RULE_PACKET_COUNT	COUNTER	False	The current number of discarded packets for the IPSEC Decrypt policer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
DISCARD_PEAK_DISCARD_RATE	GAUGE	False	The current peak discard rate for the discard rule.	True	
DISCARD_MINOR_ALARM_COUNT	GAUGE	False	The current number of minor alarms for the discard rule.	True	
DISCARD_MINOR_ALARM_DURATION	GAUGE	False	The current duration of the minor alarms in seconds for the discard rule.	True	
DISCARD_MAJOR_ALARM_COUNT	GAUGE	False	The current number of major alarms for the discard rule.	True	
DISCARD_MAJOR_ALARM_DURATION	GAUGE	False	The current duration of the major alarms in seconds for the discard rule.	True	
DECRYPT_DISCARD_PACKET_COUNT	COUNTER	False	The current number of packets discarded by SRTP decrypt discards.	True	
PEAK_DECRYPT_DISCARD_RATE	GAUGE	False	The current peak discard rate for SRTP decrypt discards.	True	
MINOR_DECRYPT_ALARM_COUNT	INTEGER	False	The current number of minor alarms for SRTP decrypt discards.	True	
MINOR_DECRYPT_ALARM_DURATION	INTEGER	False	The current duration of the minor alarms in seconds for SRTP decrypt discards.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
MAJOR_DECRYPT_ALARM_COUNT	INTEGER	False	The current number of major alarms for the SRTP decrypt discards.	True	
MAJOR_DECRYPT_ALARM_DURATION	INTEGER	False	The current duration of the major alarms in seconds for SRTP decrypt discards.	True	

CnfLinkDetectionGroupStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ACNAME	STRING	True	The name of the address context.	False	
CNF_PODNAME	STRING	True	The name of the pod.	False	
NAME	STRING	True	The name of this link detection group.	False	
SINGLE_FAILURES	INTEGER	False	The number of single failures for this link detection group.	True	
DOUBLE_FAILURES	INTEGER	False	The number of double failures for this link detection group.	True	
FAILURES	INTEGER	False	The number of failures greater than 2, for this link detection group.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfLinkMonitorStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ACNAME	STRING	True	The name of the address context.	False	
CNF_PODNAME	STRING	True	The name of the pod.	False	
GNAME	STRING	True	The name of the address context group.	False	
NAME	STRING	True	The name of the link monitor.	False	
MIN_TIME	INTEGER	False	The minimum time used to get a reply for an echo request packet.	True	
MAX_TIME	INTEGER	False	The maximum time used to get a reply for an echo request packet.	True	
AVERAGE_TIME	INTEGER	False	The average time used to get a reply for an echo request packet.	True	
SINGLE_FAILURES	INTEGER	False	The number of single failures for this IP interface.	True	
DOUBLE_FAILURES	INTEGER	False	The number of double failures for this IP interface.	True	
FAILURES	INTEGER	False	The number of failures greater than 2, for this link detection group.	True	
REPLIES	INTEGER	False	The number of replies.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
DUPLICATE_REPLIES	INTEGER	False	The number of duplicate replies.	True	
LATE_REPLIES	INTEGER	False	The number of late replies.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KAcIOffListIntStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
ROLE	INTEGER	True	Role of the system.	False	
SERIAL_INDEX	INTEGER	True	The isIndex of the system.	False	
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True	
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True	
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True	
DISCARD_COUNTER	COUNTER	False	The number of packets discarded by the policer.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KAggregateOffIntStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
ROLE	INTEGER	True	Role of the system.	False	
SERIAL_INDEX	INTEGER	True	The isIndex of the system.	False	
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True	
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True	
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True	
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KArpOffListIntStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
ROLE	INTEGER	True	Role of the system.	False	
SERIAL_INDEX	INTEGER	True	The isIndex of the system.	False	
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True	
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True	
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True	
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KBadEtherIpHdrOffIntStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
ROLE	INTEGER	True	Role of the system.	False	
SERIAL_INDEX	INTEGER	True	The isIndex of the system.	False	
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True	
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True	
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True	
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True	
ETHER_TYPE	COUNTER	False	The first etherstorageDataType found in the Ethernet packet.	True	
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KDiscardRuleOffIntStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
ROLE	INTEGER	True	Role of the system.	False	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
SERIAL_INDEX	INTEGER	True	The isIndex of the system.	False	
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True	
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True	
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True	
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True	
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KEthernetPortPacketPortStatus

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	True	The host name of the server.	False	
PORT_NAME	STRING	True	The name of the port.	False	
MAC_ADDRESS	STRING	False	The MAC address of the network interface.	False	
NEGOTIATED_SPEED	INTEGER	False	The interface speed. Packet port speed is not negotiable. When the statistics are generated for EMS, the <code>negotiatedSpeed</code> is displayed as an integer value. The possible values for <code>negotiatedSpeed</code> are: 1-speed10Mbps 2-speed100Mbps 3-speed1000Mbps 4-unknown 5-speed10000Mbps	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
LINK_STATE	INTEGER	False	The state of the interface. When the statistics are generated for EMS, the <code>linkState</code> is displayed as an integer value. The possible values for <code>linkState</code> are: 0-null 1-admnDisabled 2-admnEnabledPortDown 3-admnEnabledPortUp 4-admnDisabledNoLicense 5-admnEnabledPortDownInvalidSfpWrongSpeed 6-admnEnabledPortDownInvalidSfpNonSonus	True	
MAX_BANDWIDTH	GAUGE	False	Maximum bandwidth this port can support in bytes/sec.	True	
ALLOCATED_BANDWIDTH	GAUGE	False	Bandwidth reserved by active media streams on this port in bytes/sec.	True	
RX_BANDWIDTH	GAUGE	False	Actual Rx bandwidth in use on this port in bytes/sec.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
TX_BANDWIDTH	GAUGE	False	Actual Tx bandwidth in use on this port in bytes/sec.	True	
BANDWIDTH_USAGE	GAUGE	False	Percentage of maximum bandwidth allocated on this port.	True	
BANDWIDTH_DEVIATION	GAUGE	False	Percentage of deviation of actual bandwidth from allocated bandwidth.	True	
IF_INDEX	GAUGE	False	The unique ifIndex of this Packet NIF.	True	
AVG_RX_ACTUAL_BW	GAUGE	False	Average Incoming Bandwidth used during KPI bin interval in bytes/sec.	True	
AVG_TX_ACTUAL_BW	GAUGE	False	Average Outgoing Bandwidth used during KPI bin interval in bytes/sec.	True	
PEAK_RX_ACTUAL_BW	GAUGE	False	Peak Incoming Bandwidth used during KPI bin interval in bytes/sec.	True	
PEAK_TX_ACTUAL_BW	GAUGE	False	Peak Outgoing Bandwidth used during KPI bin interval in bytes/sec.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
AVG_RX_ACTUAL_BWUTIL	GAUGE	False	Average Incoming BW Utilization based on total available port BW instead of negotiated BW.	True	
PEAK_RX_ACTUAL_BWUTIL	GAUGE	False	Maximum Incoming BW Utilization during the KPI bin interval expressed as a percentage of the available BW.	True	
AVG_TX_ACTUAL_BWUTIL	GAUGE	False	Average Outgoing BW Utilization during the KPI bin interval based on total available BW instead of negotiated BW.	True	
PEAK_TX_ACTUAL_BWUTIL	GAUGE	False	Max Outgoing BW Utilization during the KPI bin interval expressed as a percentage of the available BW.	True	
BWALARM_THRESHOLD_EXCEEDED	GAUGE	False	Total number of times the BW alarm threshold was passed in the upward direction during the bin interval.	True	
BWALARM_CLEARED	GAUGE	False	Total number of times the BW clear alarm threshold was passed in the downward direction during the bin interval.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
AVG_USAGE_BW	GAUGE	False	Average Bandwidth Usage during KPI bin interval.	True	
PEAK_USAGE_BW	GAUGE	False	Peak Bandwidth Usage during KPI bin interval.	True	

CnfSBX5KlpSecDecryptOffIntStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
ROLE	INTEGER	True	Role of the system.	False	
SERIAL_INDEX	INTEGER	True	The isIndex of the system.	False	
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True	
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True	
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True	
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KMediaOffIntStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
ROLE	INTEGER	True	Role of the system.	False	
SERIAL_INDEX	INTEGER	True	The isIndex of the system.	False	
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True	
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True	
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True	
ETHER_TYPE	COUNTER	False	The first etherstorageDataType found in the Ethernet packet.	True	
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True	
SOURCE_UNIQUE	INTEGER	False	Determines if all discards were from a unique source address.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KRogueMediaIntStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
ROLE	INTEGER	True	Role of the system.	False	
SERIAL_INDEX	INTEGER	True	The isIndex of the system.	False	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True	
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True	
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True	
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True	
ETHER_TYPE	COUNTER	False	The first etherstorageDataType found in the ethernet packet.	True	
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True	
RING_TYPE	INTEGER	False	The media ring storageDataType.	False	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
SOURCE_UNIQUE	INTEGER	False	Determines if all discards were from a unique source address.	False	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KSiplpPeerIntervalStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
ACNAME	STRING	True	The name of the address context.	False	
ZNAME	STRING	True	The name of the address context zone.	False	
NAME	STRING	True	The name of this SIP peer group.	False	
INBOUND_SESSIONS	COUNTER	False	Indicates the total number of (interval) calls routed to this peer.	True	
INBOUND_CPS	COUNTER	False	Indicates the total number of (interval) calls routed to this peer per second.	True	
TOTAL_INBOUND_SESSIONS	COUNTER	False	Indicates the total number of (interval) inbound active sessions.	True	
OUTBOUND_SESSIONS	COUNTER	False	Indicates the total number of (interval) calls initiated by this peer.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
OUTBOUND_CPS	COUNTER	False	Indicates the total number of (interval) calls initiated by this peer per second.	True	
TOTAL_OUTBOUND_SESSIONS	COUNTER	False	Indicates the total number of (interval) outbound active sessions.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KSipOptResponseIntervalStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ACNAME	STRING	True	The name of the address context.	False	
ZNAME	STRING	True	The name of the address context zone.	False	
CNF_PODNAME	STRING	True	The name of the pod.	False	
NAME	STRING	True	The name of this SIP peer group.	False	
OPT_RESPONSE_401	COUNTER	False	Indicates the total number of (interval) 401 responses for received option messages.	True	
OPT_RESPONSE_403	COUNTER	False	Indicates the total number of (interval) 403 responses for received option messages.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
OPT_RESPONSE_407	COUNTER	False	Indicates the total number of (interval) 407 responses for received option messages.	True	
OPT_RESPONSE_481	COUNTER	False	Indicates the total number of (interval) 481 responses for received option messages.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KStrpDecryptOffIntStat

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
ROLE	INTEGER	True	Role of the system.	False	
SERIAL_INDEX	INTEGER	True	The isIndex of the system.	False	
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True	
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True	
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True	
ETHER_TYPE	COUNTER	False	The first etherstorageDataType found in the ethernet packet.	True	
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True	
SOURCE_UNIQUE	INTEGER	False	Determines if all discards were from a unique source address.	False	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSBX5KUflowOffListIntStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
ROLE	INTEGER	True	Role of the system.	False	
SERIAL_INDEX	INTEGER	True	The isIndex of the system.	False	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ADDRESS_CONTEXT	STRING	False	The name of the address context of the table entry.	True	
INTERFACE_GROUP_NAME	STRING	False	The name of the interface group of the table entry.	True	
INTERFACE_NAME	STRING	False	The name of the interface of the table entry.	True	
SOURCE_IP_ADDRESS	STRING	False	The source IP address of the table entry.	True	
DEST_IP_ADDRESS	STRING	False	The destination IP address of the table entry.	True	
SOURCE_IP_PORT	INTEGER	False	The source IP port of the table entry.	True	
DEST_IP_PORT	INTEGER	False	The destination IP port of the table entry.	True	
IP_PROTOCOL	INTEGER	False	The IP Protocol of the table entry.	True	
DISCARD_COUNT	COUNTER	False	The number of packets discarded by the policer.	True	
CE_NAME	STRING	True	The host name of the server.	False	

CnfsipOcsCallIntervalStatistics

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ACNAME	STRING	True	The name of the address context.	False	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ZNAME	STRING	True	The name of the address context zone.	False	
CNF_PODNAME	STRING	True	The name of the pod.	False	
NAME	STRING	True	The name of this SIP trunk group.	False	
ATTEMPTED_CALLS	GAUGE	False	Current Attempted OCS call statistics.	True	
RELAYED_CALLS	GAUGE	False	Current relayed OCS Invite to egress side statistics.	True	
ESTABLISHED_CALLS	GAUGE	False	Current Established OCS call statistics.	True	
SUCCESSFUL_CALLS	GAUGE	False	Current Successful OCS call statistics.	True	
FAILED_CALLS	GAUGE	False	Current Failed OCS call statistics.	True	
PENDING_CALL	GAUGE	False	Current Pending OCS call statistics.	True	
REJECTED_CALL	GAUGE	False	Current SBX Rejected OCS call statistics.	True	
CE_NAME	STRING	True	This object indicates the configured CE name.	False	

CnfSblIntervalStatistics

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
ID	GAUGE	False	Instance id Of the SIP Client.	False	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
VNFID	STRING	False	The name of the address context.	False	
MSGS_SENT	COUNTER	False	Number of messages sent to sip client.	False	
INVITE_MSGS_SENT	COUNTER	False	Number of INVITEs sent to sip client.	False	
OOD_MSGS_SENT	COUNTER	False	Number of out of dialog requests sent to sip client.	False	
REGISTER_MSG_SENT	COUNTER	False	Number of out of register requests sent to sip client.	False	
CE_NAME	STRING	True	The host name of the server.	False	

CnfSysCpuUtilIntStatsSts

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	True	This object indicates the configured CE name.	False	
CPU	GAUGE	True	The CPU number.	False	
AVERAGE	GAUGE	False	Average CPU % utilization for this interval.	True	
HIGH	GAUGE	False	High CPU % utilization for this interval.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
LOW	GAUGE	False	Low CPU % utilization for this interval.	True	

CnfSysMemoryUtilIntStatsSts

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	True	This object indicates the configured CE name.	False	
AVERAGE	GAUGE	False	The average memory % utilization for this interval.	True	
HIGH	GAUGE	False	The high memory % utilization for this interval.	True	
LOW	GAUGE	False	The low memory % utilization for this interval.	True	
AVERAGE_SWAP	GAUGE	False	The average swap memory % utilization for this interval.	True	
HIGH_SWAP	GAUGE	False	The high swap memory % utilization for this interval.	True	
LOW_SWAP	GAUGE	False	The low swap memory % utilization for this interval.	True	

CnfSystemCongestionIntervalStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
NAME	INTEGER	True	A dummy key to be added to the non-config scalar element container, although only one row is allowed in the container. Without the key, <code>tailf</code> treats the container non-dynamic and calls the <code>get_elem</code> per leaf instead of calling <code>get_object</code> per row.	False	
LEVEL_MC1_COUNT	COUNTER	False	The current number of transitions into MC1.	True	
LEVEL_MC1_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC1.	True	
LEVEL_MC2_COUNT	COUNTER	False	The current number of transitions into MC2.	True	
LEVEL_MC2_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC2.	True	
LEVEL_MC3_COUNT	COUNTER	False	The current number of transitions into MC3.	True	
LEVEL_MC3_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC3.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
OVERLOAD_REJECTS	COUNTER	False	The current number of calls rejected due to System congestion.	True	
AVG_CALL_RATE	GAUGE	False	The current system average call arrival rate.	True	
PEAK_CALL_RATE	GAUGE	False	The current system peak call arrival rate.	True	
CALL_ARRIVALS	COUNTER	False	The current number of call arrivals.	True	
EMERGENCY_CALL_ARRIVALS	COUNTER	False	The current number of SIP emergency calls arrived.	True	
EMERGENCY_CALL_REJECTS	COUNTER	False	The current number of SIP emergency calls rejected.	True	
SIP_REG_ARRIVALS	COUNTER	False	The current number of SIP registrations arrived.	True	
SIP_REG_REJECTS	COUNTER	False	The current number of SIP registrations rejected.	True	
AVG_REG_RATE	GAUGE	False	The current average SIP registration arrival rate.	True	
PEAK_REG_RATE	GAUGE	False	The current peak SIP registration arrival rate.	True	
MAX_ACTIVE_CALLS	GAUGE	False	High water mark of the total number of active calls in current interval for system level.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
SIP_SUBS_ARRIVALS	GAUGE	False	The current number of SIP subscribes arrived.	True	
SIP_SUBS_REJECTS	GAUGE	False	The current number of SIP subscribes rejected.	True	
AVG_SUBS_RATE	GAUGE	False	The current average SIP subscribe arrival rate.	True	
PEAK_SUBS_RATE	GAUGE	False	The current peak SIP subscribe arrival rate.	True	
CE_NAME	STRING	True	This object indicates the configured CE name.	False	

CnfSystemCongestionIntervalStats_AG

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
NAME	INTEGER	True	A dummy key to be added to the non-config scalar element container, although only one row is allowed in the container. Without the key, <code>tailf</code> treats the container non-dynamic and calls the <code>get_elem</code> per leaf instead of calling <code>get_object</code> per row.	False	
LEVEL_MC1_COUNT	COUNTER	False	The current number of transitions into MC1.	True	
LEVEL_MC1_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC1.	True	
LEVEL_MC2_COUNT	COUNTER	False	The current number of transitions into MC2.	True	
LEVEL_MC2_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC2.	True	
LEVEL_MC3_COUNT	COUNTER	False	The current number of transitions into MC3.	True	
LEVEL_MC3_TOTAL_TIME	COUNTER	False	The current sum of time spent in MC3.	True	
OVERLOAD_REJECTS	COUNTER	False	The current number of calls rejected due to System congestion.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
AVG_CALL_RATE	GAUGE	False	The current system average call arrival rate.	True	
PEAK_CALL_RATE	GAUGE	False	The current system peak call arrival rate.	True	
CALL_ARRIVALS	COUNTER	False	The current number of call arrivals.	True	
EMERGENCY_CALL_ARRIVALS	COUNTER	False	The current number of SIP emergency calls arrived.	True	
EMERGENCY_CALL_REJECTS	COUNTER	False	The current number of SIP emergency calls rejected.	True	
SIP_REG_ARRIVALS	COUNTER	False	The current number of SIP registrations arrived.	True	
SIP_REG_REJECTS	COUNTER	False	The current number of SIP registrations rejected.	True	
AVG_REG_RATE	GAUGE	False	The current average SIP registration arrival rate.	True	
PEAK_REG_RATE	GAUGE	False	The current peak SIP registration arrival rate.	True	
MAX_ACTIVE_CALLS	GAUGE	False	High water mark of the total number of active calls in current interval for system level.	True	
SIP_SUBS_ARRIVALS	GAUGE	False	The current number of SIP subscribes arrived.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
SIP_SUBS_REJECTS	GAUGE	False	The current number of SIP subscribes rejected.	True	
AVG_SUBS_RATE	GAUGE	False	The current average SIP subscribe arrival rate.	True	
PEAK_SUBS_RATE	GAUGE	False	The current peak SIP subscribe arrival rate.	True	
CE_NAME	STRING	True	This object indicates the configured CE name.	False	

CnfTcpGeneralGroupStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	True	This object indicates the configured CE name.	False	
ESTABLISHED_CONNECTIONS	GAUGE	False	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT. (currEstab)	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CLIENT_CONNECTIONS	COUNTER	False	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state. (activeOpens).	True	
SERVER_CONNECTIONS	COUNTER	False	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state. (passiveOpens).	True	
FAILED_ATTEMPTS	COUNTER	False	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state. (attemptFails)	True	
IN_SEGMENTS	COUNTER	False	The total number of segments received, including those received in error. This count includes segments received on currently established connections.	True	

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
OUT_SEGMENTS	COUNTER	False	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.	True	
RETRANS_SEGMENTS	COUNTER	False	The total number of segments retransmitted, that is, the number of TCP segments transmitted containing one or more previously transmitted octets.	True	
IN_ERRORS	COUNTER	False	The total number of segments received in error. For example, bad TCP checksums.	True	
IN_RESETS	COUNTER	False	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state. (estabResets)	True	
OUT_RESETS	COUNTER	False	The number of TCP segments sent containing the RST flag.	True	

CnfUdpGeneralGroupStats

Column Name	Column Type	Index	Description	Can Aggregate	CLI Command Reference
CNF_PODNAME	STRING	True	The name of the pod.	False	
CE_NAME	STRING	True	This object indicates the configured CE name.	False	
IN_DATAGRAMS	COUNTER	False	The total number of UDP datagrams delivered to UDP users.	True	
OUT_DATAGRAMS	COUNTER	False	The total number of UDP datagrams sent from this entity.	True	
UNKNOWN_PORTS	COUNTER	False	The total number of received UDP datagrams for which there was no application at the destination port.	True	
IN_ERRORS	COUNTER	False	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.	True	

DspResDspCallIntervalStats

Column Name	Column Type	Index	Description	CLI Command Reference
SYSTEM_NAME	STRING	Yes	Name of the system.	Show Table System

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_NO_DSP_ALLOC_FAIL	COUNTER	No	Number of call was successful without DSP resource allocation failure during an interval.	
NUM_CALL_WITH_DSP_ALLOC_FAIL	COUNTER	No	Number of call was successful with DSP resource allocation failure during an interval.	
NUM_CALL_FAIL_NO_G729	COUNTER	No	Number of call failed due to lack of G729 DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_G729	COUNTER	No	Number of call fails due to reason other than lack G729 DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_G729	COUNTER	No	Number of call was successful even though lack of G729 DSP resource during an interval.	
NUM_CALL_FAIL_NO_G726	COUNTER	No	Number of call failed due to lack of G726 DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_G726	COUNTER	No	Number of call fails due to reason other than lack G726 DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_G726	COUNTER	No	Number of call was successful even though lack of G726 DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_NO_G711_PACKET	COUNTER	No	Number of call failed due to lack of G711 Packet DSP resource during an interval.	
NUM_CALL_FAIL_ON_G711_PACKET	COUNTER	No	Number of call fails due to reason other than lack G711 Packet DSP resource during an interval.	
NUM_CALL_NO_G711_PACKET	COUNTER	No	Number of call was successful even though lack of G711 Packet DSP resource during an interval.	
NUM_CALL_FAIL_NO_G723	COUNTER	No	Number of call failed due to lack of G723 DSP resource during an interval.	
NUM_CALL_FAIL_ON_G723	COUNTER	No	Number of call fails due to reason other than lack G723 DSP resource during an interval.	
NUM_CALL_NO_G723	COUNTER	No	Number of call was successful even though lack of G723 DSP resource during an interval.	
NUM_CALL_FAIL_NO_ILBC	COUNTER	No	Number of call failed due to lack of ILBC DSP resource during an interval.	
NUM_CALL_FAIL_ON_ILBC	COUNTER	No	Number of call fails due to reason other than lack ILBC DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_NO_ILBC	COUNTER	No	Number of call was successful even though lack of ILBC DSP resource during an interval.	
NUM_CALL_FAIL_NO_EVRCB	COUNTER	No	Number of call failed due to lack of EVRCB0 DSP resource during an interval.	
NUM_CALL_FAIL_ON_EVRCB	COUNTER	No	Number of call fails due to reason other than lack EVRCB0 DSP resource during an interval.	
NUM_CALL_NO_EVRCB	COUNTER	No	Number of call was successful even though lack of EVRCB0 DSP resource during an interval.	
NUM_CALL_FAIL_NO_GSM	COUNTER	No	Number of call failed due to lack of AMRNB DSP resource during an interval.	
NUM_CALL_FAIL_ON_GSM	COUNTER	No	Number of call fails due to reason other than lack AMRNB DSP resource during an interval.	
NUM_CALL_NO_GSM	COUNTER	No	Number of call was successful even though lack of AMRNB DSP resource during an interval.	
NUM_CALL_FAIL_NO_AMRWB	COUNTER	No	Number of call failed due to lack of AMRWB DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_ON_AMRWB	COUNTER	No	Number of call fails due to reason other than lack AMRWB DSP resource during an interval.	
NUM_CALL_NO_AMRWB	COUNTER	No	Number of call was successful even though lack of AMRWB DSP resource during an interval.	
NUM_CALL_FAIL_NO_G722	COUNTER	No	Number of call failed due to lack of G722 DSP resource during an interval.	
NUM_CALL_FAIL_ON_G722	COUNTER	No	Number of call fails due to reason other than lack G722 DSP resource during an interval.	
NUM_CALL_NO_G722	COUNTER	No	Number of call was successful even though lack of G722 DSP resource during an interval.	
NUM_CALL_FAIL_NO_TONE	COUNTER	No	Number of call failed due to lack of TONE DSP resource during an interval.	
NUM_CALL_FAIL_ON_TONE	COUNTER	No	Number of call fails due to reason other than lack TONE DSP resource during an interval.	
NUM_CALL_NO_TONE	COUNTER	No	Number of call was successful even though lack of TONE DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_NO_EVRC	COUNTER	No	Number of call failed due to lack of EVRC DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_EVRC	COUNTER	No	Number of call fails due to reason other than lack EVRC DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_EVRC	COUNTER	No	Number of call was successful even though lack of EVRC DSP resource during an interval.	
NUM_CALL_FAIL_NO_G7221	COUNTER	No	Number of call failed due to lack of G7221 DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_G7221	COUNTER	No	Number of call fails due to reason other than lack G7221 DSP resource during an interval.	
NUM_CALL_SUCCESS_NO_G7221	COUNTER	No	Number of call was successful even though lack of G7221 DSP resource during an interval.	
NUM_CALL_FAIL_NO_EFR	COUNTER	No	Number of call failed due to lack of Efr DSP resource during an interval.	
NUM_CALL_FAIL_OTHER_ON_EFR	COUNTER	No	Number of call fails due to reason other than lack Efr DSP resource during an interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_SUC CESS_NO_EFR	COUNTER	No	Number of call was successful even though lack of Efr DSP resource during an interval.	
NUM_CALL_FAIL _NO_OPUS	COUNTER	No	Number of call failed due to lack of OPUS DSP resource during an interval.	
NUM_CALL_FAIL _OTHER_ON_OP US	COUNTER	No	Number of call fails due to reason other than lack of OPUS DSP resource during an interval.	
NUM_CALL_SUC CESS_NO_OPUS	COUNTER	No	Number of call was successful even though lack of OPUS DSP resource during an interval.	
NUM_CALL_FAIL _NO_SILK8	COUNT	No	Number of calls failed due to lack of SILK_8 DSP resource.	
NUM_CALL_FAIL _OTHER_SILK8	COUNT	No	Number of calls failed due to reason other than lack of SILK_8 DSP resource.	
NUM_CALL_SUC CESS_NO_SILK8	COUNT	No	Number of calls successful even with lack of SILK_8 DSP resource.	
NUM_CALL_FAIL _NO_SILK16	COUNT	No	Number of calls successful even with lack of SILK_8 DSP resource.	

Column Name	Column Type	Index	Description	CLI Command Reference
NUM_CALL_FAIL_OTHER_SILK16	COUNT	No	Number of calls failed due to reason other than lack of SILK_16 DSP resource.	
NUM_CALL_SUCCESS_NO_SILK16	COUNT	No	Number of calls successful even with lack of SILK_16 DSP resource.	
NUM_CALL_FAIL_NO_EVS	INTEGER	No	The number of call fails due to the lack of EVS DSP resource during a time interval.	
NUM_CALL_FAIL_OTHER_EVS	INTEGER	No	The number of call fails due to a reason other than the lack of EVS DSP resource during a time interval.	
NUM_CALL_SUCCESS_NO_EVS	INTEGER	No	The number of calls was successful despite the lack of EVS DSP resource during a time interval.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

DspResDspCallIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SYSTEM_NAME	STRING	Yes	The name of the system.	False	N/A
SUM_NUM_CALL_NO_DSP_ALLOC_FAIL	COUNTER	No	The sum of the number of successful calls without DSP resource allocation failure during an interval.	True	SUM
SUM_NUM_CALL_WITH_DSP_ALLOC_FAIL	COUNTER	No	The sum of the number of successful calls with DSP resource allocation failure during an interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_FAIL_NO_G729	COUNTER	No	The sum of the number of calls failed due to lack of G729 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_ON_G729	COUNTER	No	The sum of the number of calls failed due to reason other than lack G729 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_G729	COUNTER	No	The sum of the number of successful calls even though lack of G729 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_G726	COUNTER	No	The sum of the number of calls failed due to lack of G726 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_ON_G726	COUNTER	No	The sum of the number of calls failed due to reason other than lack G726 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_G726	COUNTER	No	The sum of the number of successful calls even though lack of G726 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_G711_PACKET	COUNTER	No	The sum of the number of calls failed due to lack of G711 Packet DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_G711_PACKET	COUNTER	No	The sum of the number of calls failed due to reason other than lack G711 Packet DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_G711_PACKET	COUNTER	No	The sum of the number of successful calls even though lack of G711 Packet DSP resource during an interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_FAIL_NO_G723	COUNTER	No	The sum of the number of calls failed due to lack of G723 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_G723	COUNTER	No	The sum of the number of calls failed due to reason other than lack G723 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_G723	COUNTER	No	The sum of the number of successful calls even though lack of G723 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_ILBC	COUNTER	No	The sum of the number of calls failed due to lack of ILBC DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_ILBC	COUNTER	No	The sum of the number of calls failed due to reason other than lack ILBC DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_ILBC	COUNTER	No	The sum of the number of successful calls even though lack of ILBC DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_EVRCB	COUNTER	No	The sum of the number of calls failed due to lack of EVRCB0 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_EVRCB	COUNTER	No	The sum of the number of calls fails due to reason other than lack EVRCB0 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_EVRCB	COUNTER	No	The sum of the number of successful calls even though lack of EVRCB0 DSP resource during an interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_FAIL_NO_GSM	COUNTER	No	The sum of the number of calls failed due to lack of AMRNB DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_GSM	COUNTER	No	The sum of the number of calls failed due to reason other than lack AMRNB DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_GSM	COUNTER	No	The sum of the number of successful calls even though lack of AMRNB DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_AMRWB	COUNTER	No	The sum of the number of calls failed due to lack of AMRWB DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_AMRWB	COUNTER	No	The sum of the number of calls failed due to reason other than lack AMRWB DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_AMRWB	COUNTER	No	The sum of the number of successful calls even though lack of AMRWB DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_G722	COUNTER	No	The sum of the number of calls failed due to lack of G722 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_G722	COUNTER	No	The sum of the number of calls failed due to reason other than lack G722 DSP resource during an interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_NO_G722	COUNTER	No	The sum of the number of successful calls even though lack of G722 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_TONE	COUNTER	No	The sum of the number of calls failed due to lack of TONE DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_ON_TONE	COUNTER	No	The sum of the number of calls failed due to reason other than lack TONE DSP resource during an interval.	True	SUM
SUM_NUM_CALL_NO_TONE	COUNTER	No	The sum of the number of successful calls even though lack of TONE DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_EVRC	COUNTER	No	The sum of the number of calls failed due to lack of EVRC DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_ON_EVRC	COUNTER	No	The sum of the number of calls failed due to reason other than lack EVRC DSP resource during an interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_EVRC	COUNTER	No	The sum of the number of successful calls even though lack of EVRC DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_EFR	COUNTER	No	The sum of the number of calls failed due to lack of Efr DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_ON_EFR	COUNTER	No	The sum of the number of calls failed due to reason other than lack Efr DSP resource during an interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_SUCCESS_NO_EFR	COUNTER	No	The sum of the number of successful calls even though lack of Efr DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_G7221	COUNTER	No	The sum of the number of calls failed due to lack of G7221 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_ON_G7221	COUNTER	No	The sum of the number of calls failed due to reason other than lack G7221 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_G7221	COUNTER	No	The sum of the number of successful calls even though lack of G7221 DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_OPUS	COUNTER	No	The sum of the number of calls failed due to lack of OPUS DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_ON_OPUS	COUNTER	No	The sum of the number of calls failed due to reason other than lack of OPUS DSP resource during an interval.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_OPUS	COUNTER	No	The sum of the number of successful calls even though lack of OPUS DSP resource during an interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_EVS	INTEGER	No	The sum of the number of calls failed due to the lack of EVS DSP resource during a time interval.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_EVS	INTEGER	No	The sum of the number of calls failed due to a reason other than the lack of EVS DSP resource during a time interval.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_CALL_SUCCESS_NO_EVS	INTEGER	No	The sum of the number of calls was successful despite the lack of EVS DSP resource during a time interval.	True	SUM
SUM_NUM_CALL_FAIL_NO_SILK8	INTEGER	No	The sum of the number of calls failed due to lack of SILK_8 DSP resource.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_SILK8	INTEGER	No	The sum of the number of calls failed due to reason other than lack of SILK_8 DSP resource.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_SILK8	INTEGER	No	The sum of the number of calls successful even with lack of SILK_8 DSP resource.	True	SUM
SUM_NUM_CALL_FAIL_NO_SILK16	INTEGER	No	The sum of the number of calls successful even with lack of SILK_8 DSP resource.	True	SUM
SUM_NUM_CALL_FAIL_OTHER_SILK16	INTEGER	No	The sum of the number of calls failed due to reason other than lack of SILK_16 DSP resource.	True	SUM
SUM_NUM_CALL_SUCCESS_NO_SILK16	INTEGER	No	The sum of the number of successful calls even with lack of SILK_16 DSP resource.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

DspResDspUsageIntervalStats

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
SYSTEM_NAME	STRING	Yes	Name of the system.		Show Table System

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G729_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G729 DSP pad during an interval time.		
G729_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G729 DSP pad during an interval time.		
G729_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G729 DSP pad during an interval time.		
G726_PEAK_USED_COUNT	GAUGE	No	The Interval number of Peak usage of type G726 DSP pad during an interval time.		
G726_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G726 DSP pad during an interval time.		
G726_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G726 DSP pad during an interval time.		
G711_PACKET_PEAK_USAGE_COUNT	GAUGE	No	The peak usage of type G711Packet DSP pad during an interval time.		
G711_PACKET_AVG_USED_COUNT	GAUGE	No	The average usage of type G711Packet DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711_PACKET_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711Packet DSP pad during an interval time.		
G723_PEAK_USED_COUNT	GAUGE	No	The Interval number of Peak usage of type G723 DSP pad during an interval time.		
G723_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G723 DSP pad during an interval time.		
G723_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G723 DSP pad during an interval time.		
ILBC_PEAK_USED_COUNT	GAUGE	No	The peak usage of type ILBC DSP pad during an interval time.		
ILBC_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type ILBC DSP pad during an interval time.		
ILBC_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type ILBC DSP pad during an interval time.		
EVRCB0_PEAK_USED_COUNT	GAUGE	No	The peak usage of type EVRCB0 DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
EVRCB0_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type EVRCB0 DSP pad during an interval time.		
EVRCB0_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type EVRCB0 DSP pad during an interval time.		
GSM_PEAK_USED_COUNT	GAUGE	No	The peak usage of type AMRNB DSP pad during an interval time.		
GSM_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type AMRNB DSP pad during an interval time.		
GSM_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type AMRNB DSP pad during an interval time.		
AMRWB_PEAK_USED_COUNT	GAUGE	No	The peak usage of type Amrwb DSP pad during an interval time.		
AMRWB_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type Amrwb DSP pad during an interval time.		
AMRWB_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type Amrwb DSP pad during an interval time.		
G722_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G722_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G722 DSP pad during an interval time.		
G722_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G722 DSP pad during an interval time.		
TONE_PEAK_USED_COUNT	GAUGE	No	The peak usage of type TONE DSP pad during an interval time.		
TONE_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type TONE DSP pad during an interval time.		
TONE_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type TONE DSP pad during an interval time.		
EVRC_PEAK_USED_COUNT	GAUGE	No	The peak usage of type EVRCB0 DSP pad during an interval time.		
EVRC_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type EVRC DSP pad during an interval time.		
EVRC_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type EVRC DSP pad during an interval time.		
G7221_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G7221 DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G7221_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G7221 DSP pad during an interval time.		
G7221_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G7221 DSP pad during an interval time.		
EFR_PEAK_USED_COUNT	GAUGE	No	The peak usage of type Efr DSP pad during an interval time.		
EFR_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type Efr DSP pad during an interval time.		
EFR_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type Efr DSP pad during an interval time.		
G711SS_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711Ss DSP pad during an interval time.		
G711SS_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G711Ss DSP pad during an interval time.		
G711SS_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G711Ss DSP pad during an interval time.		
G729V8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G729 V8 DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G729V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G729 V8 DSP pad during an interval time.		
G729V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G729 V8 DSP pad during an interval time.		
G726V8_PEAK_USED_COUNT	GAUGE	No	The Interval number of Peak usage of type G726 V8 DSP pad during an interval time.		
G726V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G726 V8 DSP pad during an interval time.		
G726V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G726 V8 DSP pad during an interval time.		
G711V8_PACKET_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711Packet V8 DSP pad during an interval time.		
G711V8_PACKET_AVG_USED_COUNT	GAUGE	No	The average usage of type G711Packet V8 DSP pad during an interval time.		
G711V8_PACKET_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711Packet V8 DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SSV8_P EAK_USED_ COUNT	GAUGE	No	The peak usage of type G711SSPacket V8 DSP pad during an interval time.		
G711SSV8_A VERAGE_US ED_COUNT	GAUGE	No	The average usage of type G711SSPacket V8 DSP pad during an interval time.		
G711SSV8_A VERAGE_AVA IL_COUNT	GAUGE	No	The average availability of type G711SSPacket V8 DSP pad during an interval time.		
G723V8_PEA K_USED_CO UNT	GAUGE	No	The Interval number of Peak usage of type G723 V8 DSP pad during an interval time.		
G723V8_AVE RAGE_USED _COUNT	GAUGE	No	The average usage of type G723 V8 DSP pad during an interval time.		
G723V8_AVE RAGE_AVAIL _COUNT	GAUGE	No	The average availability of type G723 V8 DSP pad during an interval time.		
ILBCV8_PEA K_USED_CO UNT	GAUGE	No	The peak usage of type ILBC V8 DSP pad during an interval time.		
ILBCV8_AVE RAGE_USED _COUNT	GAUGE	No	The average usage of type ILBC V8 DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
ILBCV8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type ILBC V8 DSP pad during an interval time.		
G722V8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 V8 DSP pad during an interval time.		
G722V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G722 V8 DSP pad during an interval time.		
G722V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G722 V8 DSP pad during an interval time.		
G7221V8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722.1 V8 DSP pad during an interval time.		
G7221V8_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type G722.1 V8 DSP pad during an interval time.		
G7221V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type G722.1 V8 DSP pad during an interval time.		
OPUS_PEAK_USED_COUNT	GAUGE	No	The peak usage of type OPUS DSP pad during an interval time.		
OPUS_AVERAGE_USED_COUNT	GAUGE	No	The average usage of type OPUS DSP pad during an interval time.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
OPUS_AVERAGE_AVAIL_COUNT	GAUGE	No	The average availability of type OPUS DSP pad during an interval time.		
EVS_PEAK_USED_COUNT	GAUGE	No	The peak usage of type EVS DSP pad during an interval time.		
EVS_AVG_USED_COUNT	GAUGE	No	The average usage of type EVS DSP pad during an interval time.		
EVS_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type EVS DSP pad during an interval time.		
SILK8_PEAK_USED_COUNT	COUNT	No	The peak usage of type SILK_8 DSP PAD.		
SILK8_AVG_USED_COUNT	COUNT	No	The average usage of type SILK_8 DSP PAD.		
SILK8_AVG_AVAIL_COUNT	COUNT	No	The average availability of type SILK_8 DSP PAD.		
SILK16_PEAK_USED_COUNT	COUNT	No	The peak usage of type SILK_16 DSP PAD.		
SILK16_AVG_USED_COUNT	COUNT	No	The average usage of type SILK_16 DSP PAD.		
SILK16_AVG_AVAIL_COUNT	COUNT	No	The average availability of type SILK_16 DSP PAD.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
AMRWT140_ PEAK_USED_ COUNT	COUNT	No	The peak usage of type AMR with T.140 DSP pad during an interval time.		
AMRWT140_ AVG_USED_ COUNT	COUNT	No	The peak usage of type AMR with T.140 DSP pad during an interval time.		
AMRWT140_ AVG_AVAIL_ COUNT	COUNT	No	The average availability of type AMR with T.140 DSP pad during an interval time.		
AMRWBT140_ PEAK_USED_ COUNT	COUNT	No	The peak usage of type AMRWB with T.140 DSP pad during an interval time.		
AMRWBT140_ AVG_USED_ COUNT	COUNT	No	The average usage of type SILK_16 DSP pad during an interval time.		
AMRWBT140_ AVG_AVAIL_ COUNT	COUNT	No	The average availability of type SILK_16 DSP pad during an interval time.		
AMR_PEAK_ USAGE_ COUNT	GAUGE	No	The current peak usage of type AMRNB DSP PAD.		
AMR_AVG_ USAGE_ COUNT	GAUGE	No	The current average usage of type AMRNB DSP PAD.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
AMR_AVG_A VAIL_COUNT	GAUGE	No	The current average availability of type AMRNB DSP PAD.		
EVS_T140_P EAK_USED_ COUNT	GAUGE	No	The peak usage of type EVS with T.140 DSP pad during an interval time.		
EVS_T140_A VERAGE_US ED_COUNT	GAUGE	No	The average usage of type EVS with T.140 DSP pad during an interval time.		
EVS_T140_A VERAGE_AVA IL_COUNT	GAUGE	No	The average availability of type EVS with T.140 DSP pad during an interval time.		
G711T140_PE AK_USED_C OUNT	GAUGE	No	The average availability of type EVS with T.140 DSP pad during an interval time.	MEAN	
G711T140_AV G_USED_CO UNT	GAUGE	No	The average usage of type G711 with T.140 DSP pad during an interval time.	MEAN	
G711T140_AV G_AVAIL_CO UNT	GAUGE	No	The average availability of type G711 with T.140 DSP pad during an interval time.	MEAN	
G711SST140_ PEAK_USED_ COUNT	GAUGE	No	The peak usage of type G711SS with T.140 DSP pad during an interval time.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SST140_AVG_USED_COUNT	GAUGE	No	The average usage of type G711SS with T.140 DSP pad during an interval time.	MEAN	
G711SST140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711SS with T.140 DSP pad during an interval time.	MEAN	
OPUST140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type Opus with T.140 DSP pad during an interval time.	MEAN	
OPUST140_AVG_USED_COUNT	GAUGE	No	The average usage of type Opus with T.140 DSP pad during an interval time.	MEAN	
OPUST140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type Opus with T.140 DSP pad during an interval time.	MEAN	
G722T140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 with T.140 DSP pad during an interval time.	MEAN	
G722T140_AVG_USED_COUNT	GAUGE	No	The average usage of type G722 with T.140 DSP pad during an interval time.	MEAN	
G722T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G722 with T.140 DSP pad during an interval time.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G722V8T140_ PEAK_USED_ COUNT	GAUGE	No	The peak usage of type G722 V8 with T.140 DSP pad during an interval time.	MEAN	
G722V8T140_ AVG_USED_ COUNT	GAUGE	No	The average usage of type G722 V8 with T.140 DSP pad during an interval time.	MEAN	
G722V8T140_ AVG_AVAIL_ COUNT	GAUGE	No	The average availability of type G722 V8 with T.140 DSP pad during an interval time.	MEAN	
G711T140V8_ PEAK_USED_ COUNT	GAUGE	No	The peak usage of type G711 V8 with T.140 DSP pad during an interval time.	MEAN	
G711T140V8_ AVG_USED_ COUNT	GAUGE	No	The average usage of type G711 V8 with T.140 DSP pad during an interval time.	MEAN	
G711T140V8_ AVG_AVAIL_ COUNT	GAUGE	No	The average availability of type G711 V8 with T.140 DSP pad during an interval time.	MEAN	
G711SSV8T140_ PEAK_USED_ COUNT	GAUGE	No	The peak usage of type G711SS V8 with T.140 DSP pad during an interval time.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SSV8T140_AVG_USAGE_COUNT	GAUGE	No	The average usage of type G711SS V8 with T.140 DSP pad during an interval time.	MEAN	
G711SSV8T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711SS V8 with T.140 DSP pad during an interval time.	MEAN	
L16_PEAK_USAGE_COUNT	GAUGE	No	The peak usage of type L16 DSP pad during an interval time.	MEAN	
L16_AVG_USAGE_COUNT	GAUGE	No	The average usage of type L16 DSP pad during an interval time.	MEAN	
L16_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type L16 DSP pad during an interval time.	MEAN	
CE_NAME	STRING	No	The name of the compute element for this entry.	N/A	

DspResDspUsageIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SYSTEM_NAME	STRING	Yes	Name of the system.	False	N/A
AVG_G729_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G729 DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_G729_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G729 DSP pad during an interval time.	True	AVG
AVG_G729_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G729 DSP pad during an interval time.	True	AVG
AVG_G726_PEAK_USED_COUNT	GAUGE	No	The average of interval number of Peak usage of type G726 DSP pad during an interval time.i	True	AVG
AVG_G726_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G726 DSP pad during an interval time.	True	AVG
AVG_G726_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G726 DSP pad during an interval time.	True	AVG
AVG_G711_PACKET_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G711Packet DSP pad during an interval time.	True	AVG
AVG_G711_PACKET_AVG_USED_COUNT	GAUGE	No	The average of average usage of type G711Packet DSP pad during an interval time.	True	AVG
AVG_G711_PACKET_AVG_AVAIL_COUNT	GAUGE	No	The average of average availability of type G711Packet DSP pad during an interval time.	True	AVG
AVG_G723_PEAK_USED_COUNT	GAUGE	No	The average of interval number of Peak usage of type G723 DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_G723_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G723 DSP pad during an interval time.	True	AVG
AVG_G723_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G723 DSP pad during an interval time.	True	AVG
AVG_ILBC_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type ILBC DSP pad during an interval time.	True	AVG
AVG_ILBC_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type ILBC DSP pad during an interval time.	True	AVG
AVG_ILBC_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type ILBC DSP pad during an interval time.	True	AVG
AVG_EVRCB0_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type EVRCB0 DSP pad during an interval time.	True	AVG
AVG_EVRCB0_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type EVRCB0 DSP pad during an interval time.	True	AVG
AVG_EVRCB0_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type EVRCB0 DSP pad during an interval time.	True	AVG
AVG_GSM_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type AMRNB DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_GSM_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type AMRNB DSP pad during an interval time.	True	AVG
AVG_GSM_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type AMRNB DSP pad during an interval time.	True	AVG
AVG_AMRWB_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type Amrwb DSP pad during an interval time.	True	AVG
AVG_AMRWB_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type Amrwb DSP pad during an interval time.	True	AVG
AVG_AMRWB_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type Amrwb DSP pad during an interval time.	True	AVG
AVG_G722_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G722 DSP pad during an interval time.	True	AVG
AVG_G722_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G722 DSP pad during an interval time.	True	AVG
AVG_G722_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G722 DSP pad during an interval time.	True	AVG
AVG_TONE_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type TONE DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_TONE_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type TONE DSP pad during an interval time.	True	AVG
AVG_TONE_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type TONE DSP pad during an interval time.	True	AVG
AVG_EVRC_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type EVRCB0 DSP pad during an interval time.	True	AVG
AVG_EVRC_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type EVRC DSP pad during an interval time.	True	AVG
AVG_EVRC_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type EVRC DSP pad during an interval time.	True	AVG
AVG_G7221_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G7221 DSP pad during an interval time.	True	AVG
AVG_G7221_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G7221 DSP pad during an interval time.	True	AVG
AVG_G7221_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G7221 DSP pad during an interval time.	True	AVG
AVG_EFR_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type Efr DSP pad during an interval time.	True	AVG
AVG_EFR_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type Efr DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_EFR_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type Efr DSP pad during an interval time.	True	AVG
AVG_G711SS_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G711Ss DSP pad during an interval time.	True	AVG
AVG_G711SS_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G711Ss DSP pad during an interval time.	True	AVG
AVG_G711SS_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G711Ss DSP pad during an interval time.	True	AVG
AVG_G729V8_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G729 V8 DSP pad during an interval time.	True	AVG
AVG_G729V8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G729 V8 DSP pad during an interval time.	True	AVG
AVG_G729V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G729 V8 DSP pad during an interval time.	True	AVG
AVG_G726V8_PEAK_USED_COUNT	GAUGE	No	The average of interval number of Peak usage of type G726 V8 DSP pad during an interval time.	True	AVG
AVG_G726V8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G726 V8 DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_G726V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G726 V8 DSP pad during an interval time.	True	AVG
AVG_G711V8_PACKET_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G711Packet V8 DSP pad during an interval time.	True	AVG
AVG_G711V8_PACKET_AVG_USED_COUNT	GAUGE	No	The average of average usage of type G711Packet V8 DSP pad during an interval time.	True	AVG
AVG_G711V8_PACKET_AVG_AVAIL_COUNT	GAUGE	No	The average of average availability of type G711Packet V8 DSP pad during an interval time.	True	AVG
AVG_G711SSV8_PACKET_USED_COUNT	GAUGE	No	The average of peak usage of type G711SSPacket V8 DSP pad during an interval time.	True	AVG
AVG_G711SSV8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G711SSPacket V8 DSP pad during an interval time.	True	AVG
AVG_G711SSV8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G711SSPacket V8 DSP pad during an interval time.	True	AVG
AVG_G723V8_PACKET_USED_COUNT	GAUGE	No	The average of interval number of Peak usage of type G723 V8 DSP pad during an interval time.	True	AVG
AVG_G723V8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G723 V8 DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_G723V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G723 V8 DSP pad during an interval time.	True	AVG
AVG_ILBCV8_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type ILBC V8 DSP pad during an interval time.	True	AVG
AVG_ILBCV8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type ILBC V8 DSP pad during an interval time.	True	AVG
AVG_ILBCV8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type ILBC V8 DSP pad during an interval time.	True	AVG
AVG_G722V8_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G722 V8 DSP pad during an interval time.	True	AVG
AVG_G722V8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G722 V8 DSP pad during an interval time.	True	AVG
AVG_G722V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G722 V8 DSP pad during an interval time.	True	AVG
AVG_G7221V8_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type G722.1 V8 DSP pad during an interval time.	True	AVG
AVG_G7221V8_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type G722.1 V8 DSP pad during an interval time.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_G7221V8_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type G722.1 V8 DSP pad during an interval time.	True	AVG
AVG_OPUS_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type OPUS DSP pad during an interval time.	True	AVG
AVG_OPUS_AVERAGE_USED_COUNT	GAUGE	No	The average of average usage of type OPUS DSP pad during an interval time.	True	AVG
AVG_OPUS_AVERAGE_AVAIL_COUNT	GAUGE	No	The average of average availability of type OPUS DSP pad during an interval time.	True	AVG
AVG_EVS_PEAK_USED_COUNT	GAUGE	No	The average of peak usage of type EVS DSP pad during an interval time.	True	AVG
AVG_EVS_AVG_USED_COUNT	GAUGE	No	The average of average usage of type EVS DSP pad during an interval time.	True	AVG
AVG_EVS_AVG_AVAIL_COUNT	GAUGE	No	The average of average availability of type EVS DSP pad during an interval time.	True	AVG
AVG_SILK8_PEAK_USED_COUNT	COUNT	No	The average of peak usage of type SILK_8 DSP PAD.	True	AVG
AVG_SILK8_AVG_USED_COUNT	COUNT	No	The average of average usage of type SILK_8 DSP PAD.	True	AVG
AVG_SILK8_AVG_AVAIL_COUNT	COUNT	No	The average of average availability of type SILK_8 DSP PAD.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_SILK16_PEAK_USED_COUNT	COUNT	No	The average of peak usage of type SILK_16 DSP PAD.	True	AVG
AVG_SILK16_AVG_USED_COUNT	COUNT	No	The average of average usage of type SILK_16 DSP PAD.	True	AVG
AVG_SILK16_AVG_AVAIL_COUNT	COUNT	No	The average of average availability of type SILK_16 DSP PAD.	True	AVG
AVG_AMRWT140_PEAK_USED_COUNT	COUNT	No	The average of peak usage of type AMR with T.140 DSP pad during an interval time.	True	AVG
AVG_AMRWT140_AVG_USED_COUNT	COUNT	No	The average of average usage of type AMR with T.140 DSP pad during an interval time.	True	AVG
AVG_AMRWT140_AVG_AVAIL_COUNT	COUNT	No	The average of average availability of type AMR with T.140 DSP pad during an interval time.	True	AVG
AVG_AMRWBT140_PEAK_USED_COUNT	COUNT	No	The average of peak usage of type AMRWB with T.140 DSP pad during an interval time.	True	AVG
AVG_AMRWBT140_AVG_USED_COUNT	COUNT	No	The average of average usage of type SILK_16 DSP pad during an interval time.	True	AVG
AVG_AMRWBT140_AVG_AVAIL_COUNT	COUNT	No	The average of average availability of type SILK_16 DSP pad during an interval time.	True	AVG
AVG_AMR_PEAK_USAGE_COUNT	GAUGE	No	The current peak usage of type AMRNB DSP PAD.	True	MEAN

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_AMR_AVG_USAGE_COUNT	GAUGE	No	The current average usage of type AMRNB DSP PAD.	True	MEAN
AVG_AMR_AVG_AVAIL_COUNT	GAUGE	False	The current average availability of type AMRNB DSP PAD.	True	MEAN
EVS_T140_PEAK_USED_COUNT	GAUGE	False	The peak usage of type EVS with T.140 DSP pad during an interval time.	True	MEAN
EVS_T140_AVERAGE_USED_COUNT	GAUGE	False	The average usage of type EVS with T.140 DSP pad during an interval time.	True	MEAN
EVS_T140_AVERAGE_AVAIL_COUNT	GAUGE	False	The average availability of type EVS with T.140 DSP pad during an interval time.	True	MEAN
G711T140_PEAK_USED_COUNT	GAUGE	No	The average availability of type EVS with T.140 DSP pad during an interval time.	True	MEAN
G711T140_AVG_USAGE_COUNT	GAUGE	No	The average usage of type G711 with T.140 DSP pad during an interval time.	True	MEAN
G711T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711 with T.140 DSP pad during an interval time.	True	MEAN
G711SST140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711SS with T.140 DSP pad during an interval time.	True	MEAN
G711SST140_AVG_USAGE_COUNT	GAUGE	No	The average usage of type G711SS with T.140 DSP pad during an interval time.	True	MEAN

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
G711SST140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711SS with T.140 DSP pad during an interval time.	True	MEAN
OPUST140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type Opus with T.140 DSP pad during an interval time.	True	MEAN
OPUST140_AVG_USED_COUNT	GAUGE	No	The average usage of type Opus with T.140 DSP pad during an interval time.	True	MEAN
OPUST140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type Opus with T.140 DSP pad during an interval time.	True	MEAN
G722T140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 with T.140 DSP pad during an interval time.	True	MEAN
G722T140_AVG_USED_COUNT	GAUGE	No	The average usage of type G722 with T.140 DSP pad during an interval time.	True	MEAN
G722T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G722 with T.140 DSP pad during an interval time.	True	MEAN
G722V8T140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G722 V8 with T.140 DSP pad during an interval time.	True	MEAN
G722V8T140_AVG_USED_COUNT	GAUGE	No	The average usage of type G722 V8 with T.140 DSP pad during an interval time.	True	MEAN
G722V8T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G722 V8 with T.140 DSP pad during an interval time.	True	MEAN

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
G711T140V8_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711 V8 with T.140 DSP pad during an interval time.	True	MEAN
G711T140V8_AVG_USED_COUNT	GAUGE	No	The average usage of type G711 V8 with T.140 DSP pad during an interval time.	True	MEAN
G711T140V8_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711 V8 with T.140 DSP pad during an interval time.	True	MEAN
G711SSV8T140_PEAK_USED_COUNT	GAUGE	No	The peak usage of type G711SS V8 with T.140 DSP pad during an interval time.	True	MEAN
G711SSV8T140_AVG_USED_COUNT	GAUGE	No	The average usage of type G711SS V8 with T.140 DSP pad during an interval time.	True	MEAN
G711SSV8T140_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type G711SS V8 with T.140 DSP pad during an interval time.	True	MEAN
L16_PEAK_USED_COUNT	GAUGE	No	The peak usage of type L16 DSP pad during an interval time.	True	MEAN
L16_AVG_USED_COUNT	GAUGE	No	The average usage of type L16 DSP pad during an interval time.	True	MEAN
L16_AVG_AVAIL_COUNT	GAUGE	No	The average availability of type L16 DSP pad during an interval time.	True	MEAN
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

EthernetPortMgmtStats

Column Name	Column Type	Index	Description	CLI Command Reference
PORT_NAME	STRING	Yes	The name of this port.	Ethernet Port - CLI
RX_PACKETS	COUNTER64	No	The number of received packets.	
TX_PACKETS	COUNTER64	No	The number of transmitted packets.	
RX_ERRORS	COUNTER	No	The number of bad packets received.	
TX_ERRORS	COUNTER	No	The number of packet transmit failures.	
RX_DROPPED	COUNTER	No	The number of packets dropped due to no receive buffers.	
TX_DROPPED	COUNTER	No	The number of packets dropped due to no transmit buffers.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

NBS5200CallCountStats

Column Name	Column Type	Index	Description	CLI Command Reference
KEY	IMPLIEDSTRING	Yes	Key value for the call.	Show Table System
CALL_ATTEMPTS	COUNTER	No	Number of call attempts on this server.	
CALL_COMPLETIONS	COUNTER	No	Total number of completed call attempts on this server.	
ACTIVE_CALLS	GAUGE	No	Current number of active managed calls on this server.	

Column Name	Column Type	Index	Description	CLI Command Reference
STABLE_CALLS	GAUGE	No	Current number of stable managed calls on this server.	
MAX_LICENSE_LIMIT	INTEGER	No	This object indicates maximum license limit of this server.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

NBS5200CallCountStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
KEY	IMPLIEDSTRING	Yes	Key value for the call.	False	N/A
CALL_ATTEMPTS	COUNTER	No	Number of call attempts on this server.	True	SUM
CALL_COMPLETIONS	COUNTER	No	Total number of completed call attempts on this server.	True	SUM
ACTIVE_CALLS	GAUGE	No	Current number of active managed calls on this server.	False	MEAN
AVG_STABLE_CALLS	GAUGE	No	Current number of stable managed calls on this server.	False	MEAN
AVG_MAX_LICENSE_LIMIT	INTEGER	No	The average of maximum license limit of this server.	True	MEAN
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

NBS5200TGStatusStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of this Address Context.	False	N/A
ZNAME	STRING	Yes	The name of the address context zone.	False	N/A
NAME	STRING	Yes	The name of this IP trunk group.	False	N/A
AVG_STATE	INTEGER	No	The average of the current operational state of the IP trunk group.	True	AVG
AVG_TOTAL_CALLS_AVAILABLE	GAUGE	No	The average of the sum of all available or unblocked calls for this trunk group.	True	AVG
AVG_TOTAL_CALLS_INBOUND_RESERVED	GAUGE	No	The average of the reserved count as specified by the percentage configured for this IP trunk group. This object shows the total number of calls that are reserved for inbound calls on this IP trunk group. This is applicable only for IP trunk groups that are configured for inbound or both directions.	True	AVG
AVG_INBOUND_CALLS_USAGE	GAUGE	No	The average of the current inbound or incoming usage count of this IP trunk group. This is applicable only for IP trunk groups that are configured for inbound or both directions.	True	AVG
AVG_OUTBOUND_CALLS_USAGE	GAUGE	No	The average of the current outbound, non-priority usage count of this IP trunk group.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_TOTAL_CALLS_CONFIGURED	GAUGE	No	The average of the total number of calls that are configured on this IP trunk group.	True	AVG
AVG_TG_UTIL_PERCENT	INTEGER	No	This is calculated as: $\left(\frac{((\text{PSTN\_INBOUND\_USAGE} + \text{PSTN\_OUTBOUND\_USAGE}) * 100)}{\text{PSTN\_TOTAL\_CONFIGURED}} \right)$	True	AVG
AVG_PRIORITY_CALL_USAGE	GAUGE	No	The average of the current priority usage count of this IP trunk group. This is applicable for IP trunk groups that are configured with call reserved state enabled.	True	AVG
AVG_TOTAL_OUTBOUND_CALLS_RESERVED	GAUGE	No	The average of the reserved count as specified by the percentage configured for this IP trunk group. This object reflects the total number of calls that are reserved for outbound calls on this IP trunk group. This is applicable for IP trunk groups that are configured for incoming call reservation.	True	AVG
AVG_BW_CURRENT_LIMIT	INTEGER	No	The average of the current bandwidth limit for this IP trunk group. It is initially set to the configured bandwidth limit but the packet outage detection events may reduce this limit.	True	AVG
AVG_BW_AVAILABLE	INTEGER	No	The average of the bandwidth available for allocation.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
AVG_BW_INBOUND_USAGE	GAUGE	No	The average of the bandwidth in use for inbound traffic.	True	AVG
AVG_BW_OUTBOUND_USAGE	GAUGE	No	The average of the bandwidth in use for outbound traffic.	True	AVG
AVG_PACKET_OUT_DETECT_STATE	INTEGER	No	This average of the packet outage detection state. • normal - No packet outage is declared • packetOutageState - Packet outage is declared The packet outage detection bandwidth limit reduction reduces the current bandwidth limit.	True	AVG
AVG_PRIORITY_BW_USAGE	GAUGE	No	The average of the current media bandwidth in use for oversubscribed HPC/emergency calls (in Kbits/sec).	True	AVG
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

NBS5200TrunkGroupStatusStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of this Address Context.	Show Table System
ZNAME	STRING	Yes	The name of the address context zone.	
NAME	STRING	Yes	The name of this IP trunk group.	
STATE	INTEGER	No	Current operational state of the IP trunk group.	
TOTAL_CALLS_AVAILABLE	GAUGE	No	The sum of all available or unblocked calls for this trunk group.	

Column Name	Column Type	Index	Description	CLI Command Reference
TOTAL_CALLS_INBOUND_RESERVED	GAUGE	No	The reserved count as specified by the percentage configured for this IP trunk group. This object shows the total number of calls that are reserved for inbound calls on this IP trunk group. This is applicable only for IP trunk groups that are configured for inbound or both directions.	
INBOUND_CALLS_USAGE	GAUGE	No	The current inbound or incoming usage count of this IP trunk group. This is applicable only for IP trunk groups that are configured for inbound or both directions.	
OUTBOUND_CALLS_USAGE	GAUGE	No	The current outbound, non-priority usage count of this IP trunk group.	
TOTAL_CALLS_CONFIGURED	GAUGE	No	The total number of calls that are configured on this IP trunk group.	
TG_UTIL_PERCENT	INTEGER	No	This is calculated as: $\left(\frac{((\text{PSTN\_INBOUND\_USAGE} + \text{PSTN\_OUTBOUND\_USAGE}) * 100)}{\text{PSTN\_TOTAL\_CONFIGURED}} \right)$	
PRIORITY_CALL_USAGE	GAUGE	No	The current priority usage count of this IP trunk group. This is applicable for IP trunk groups that are configured with call reserved state enabled.	

Column Name	Column Type	Index	Description	CLI Command Reference
TOTAL_OUTBOUND_CALLS_RESERVED	GAUGE	No	The reserved count as specified by the percentage configured for this IP trunk group. This object reflects the total number of calls that are reserved for outbound calls on this IP trunk group. This is applicable for IP trunk groups that are configured for incoming call reservation.	
BW_CURRENT_LIMIT	INTEGER	No	The current bandwidth limit for this IP trunk group. It is initially set to the configured bandwidth limit but the packet outage detection events may reduce the limit.	
BW_AVAILABLE	INTEGER	No	Bandwidth available for allocation.	
BW_INBOUND_USAGE	GAUGE	No	Bandwidth in use for inbound traffic.	
BW_OUTBOUND_USAGE	GAUGE	No	Bandwidth in use for outbound traffic.	
PACKET_OUTAGE_DETECTION_STATE	INTEGER	No	This object indicates the packet outage detection state. • normal - No packet outage is declared • packetOutageState - Packet outage is declared The packet outage detection bandwidth limit reduction reduces the current bandwidth limit.	

Column Name	Column Type	Index	Description	CLI Command Reference
PRIORITY_BW_USAGE	GAUGE	No	The current media bandwidth in use for oversubscribed HPC/ emergency calls (in Kbits/ sec).	
CE_NAME	STRING	No	The name of the compute element for this entry.	

SBCCOREOodMessageIntStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
NAME	STRING	True	The name of this SIP IP Peer.	False	N/A
MESSAGE_RATE	COUNT	False	Number of incoming OOD requests received per second.	False	N/A
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBCCORESipRegCountDomIntStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	true	The name of the address context.	false
DOMAIN_NAME	STRING	true	Domain name of the registration.	false
COUNT_ATTEMPTS	COUNTER	true	The number of SIP registration attempts.	false
COUNTCUM_COMPLETED	COUNTER	false	The accumulative number of completed SIP registration attempts.	true
COUNT_PENDING	COUNTER	false	The current number of pending SIP registrations.	true

Column Name	Column Type	Index	Description	canAggregate
COUNT_STABLE	COUNTER	false	The current number of stable SIP registrations.	true
COUNT_TOTAL	COUNTER	false	The total number of current SIP registrations.	true
EMERGENCY_ACC_TOT	COUNTER	false	The total number of accepted emergency SIP registrations.	true
EMERGENCY_COUNT_ACT	COUNTER	false	The total number of active emergency SIP registrations.	true
CE_NAME	STRING	False	The name of the compute element for this entry.	false

SBCCORESipRegCountDomIntStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
ACNAME	STRING	true	The name of the address context.	false	N/A
DOMAIN_NAME	STRING	true	Domain name of the registration.	false	N/A
COUNT_ATTEMPTS	COUNTER	true	The number of SIP registration attempts.	false	N/A
SUM_COUNTCUM_COMPLETED	COUNTER	false	The accumulative number of completed SIP registration attempts.	true	SUM
SUM_COUNT_PENDING	COUNTER	false	The current number of pending SIP registrations.	true	SUM
SUM_COUNT_STABLE	COUNTER	false	The current number of stable SIP registrations.	true	SUM
SUM_COUNT_TOTAL	COUNTER	false	The total number of current SIP registrations.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_EMERGENCY_ACC_TOT	COUNTER	false	The total number of accepted emergency SIP registrations.	true	SUM
SUM_EMERGENCY_COUNT_ACT	COUNTER	false	The total number of active emergency SIP registrations.	true	SUM
CE_NAME	STRING	false	The name of the compute element for this entry.	false	N/A

SBCCORESipTgCSSRIntStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	true	The name of the address context.	false
ZNAME	STRING	true	The name of the address context zone.	false
NAME	STRING	true	The name of this SIP trunk group.	false
INV_SENT	COUNTER	false	The total number of (interval) inv_sent.	true
INV_RCVD	COUNTER	false	The total number of (interval) inv_rcvd.	true
ALERT_SENT	COUNTER	false	The total number of (interval) 18x_sent.	true
ALERT_RCVD	COUNTER	false	The total number of (interval) 18x_rcvd.	true
ANSCALLS_SENT	COUNTER	false	The total number of (interval) ansCalls_sent.	true
ANSCALLS_RCVD	COUNTER	false	The total number of (interval) ansCalls_rcvd.	true
CANCEL_SENT	COUNTER	false	The total number of (interval) cancel_sent.	true

Column Name	Column Type	Index	Description	canAggregate
CANCEL_RCVD	COUNTER	false	The total number of (interval) cancel_rcvd.	true
BYE_SENT	COUNTER	false	The total number of (interval) bye_sent.	true
BYE_RCVD	COUNTER	false	The total number of (interval) bye_rcvd.	true
INV200_SENT	COUNTER	false	The total number of (interval) inv200_sent.	true
INV200_RCVD	COUNTER	false	The total number of (interval) inv200_rcvd.	true
INV380_SENT	COUNTER	false	The total number of (interval) inv380_sent.	true
INV380_RCVD	COUNTER	false	The total number of (interval) inv380_rcvd.	true
INV400_SENT	COUNTER	false	The total number of (interval) inv400_sent.	true
INV400_RCVD	COUNTER	false	The total number of (interval) inv400_rcvd.	true
INV403_SENT	COUNTER	false	The total number of (interval) inv403_sent.	true
INV403_RCVD	COUNTER	false	The total number of (interval) inv403_rcvd.	true
INV404_SENT	COUNTER	false	The total number of (interval) inv404_sent.	true
INV404_RCVD	COUNTER	false	The total number of (interval) inv404_rcvd.	true
INV406_SENT	COUNTER	false	The total number of (interval) inv406_sent.	true
INV406_RCVD	COUNTER	false	The total number of (interval) inv406_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
INV408_SENT	COUNTER	false	The total number of (interval) inv408_sent.	true
INV408_RCVD	COUNTER	false	The total number of (interval) inv408_rcvd.	true
INV410_SENT	COUNTER	false	The total number of (interval) inv410_sent.	true
INV410_RCVD	COUNTER	false	The total number of (interval) inv410_rcvd.	true
INV420_SENT	COUNTER	false	The total number of (interval) inv420_sent.	true
INV420_RCVD	COUNTER	false	The total number of (interval) inv420_rcvd.	true
INV480_SENT	COUNTER	false	The total number of (interval) inv480_sent.	true
INV480_RCVD	COUNTER	false	The total number of (interval) inv480_rcvd.	true
INV481_SENT	COUNTER	false	The total number of (interval) inv481_sent.	true
INV481_RCVD	COUNTER	false	The total number of (interval) inv481_rcvd.	true
INV482_SENT	COUNTER	false	The total number of (interval) inv482_sent.	true
INV482_RCVD	COUNTER	false	The total number of (interval) inv482_rcvd.	true
INV483_SENT	COUNTER	false	The total number of (interval) inv483_sent.	true
INV483_RCVD	COUNTER	false	The total number of (interval) inv483_rcvd.	true
INV484_SENT	COUNTER	false	The total number of (interval) inv484_sent.	true

Column Name	Column Type	Index	Description	canAggregate
INV484_RCVD	COUNTER	false	The total number of (interval) inv484_rcvd.	true
INV486_SENT	COUNTER	false	The total number of (interval) inv486_sent.	true
INV486_RCVD	COUNTER	false	The total number of (interval) inv486_rcvd.	true
INV487_SENT	COUNTER	false	The total number of (interval) inv487_sent.	true
INV487_RCVD	COUNTER	false	The total number of (interval) inv487_rcvd.	true
INV488_SENT	COUNTER	false	The total number of (interval) inv488_sent.	true
INV488_RCVD	COUNTER	false	The total number of (interval) inv488_rcvd.	true
INV500_SENT	COUNTER	false	The total number of (interval) inv500_sent.	true
INV500_RCVD	COUNTER	false	The total number of (interval) inv500_rcvd.	true
INV501_SENT	COUNTER	false	The total number of (interval) inv501_sent.	true
INV501_RCVD	COUNTER	false	The total number of (interval) inv501_rcvd.	true
INV502_SENT	COUNTER	false	The total number of (interval) inv502_sent.	true
INV502_RCVD	COUNTER	false	The total number of (interval) inv502_rcvd.	true
INV503_SENT	COUNTER	false	The total number of (interval) inv503_sent.	true
INV503_RCVD	COUNTER	false	The total number of (interval) inv503_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
INV504_SENT	COUNTER	false	The total number of (interval) inv504_sent.	true
INV504_RCVD	COUNTER	false	The total number of (interval) inv504_rcvd.	true
INV580_SENT	COUNTER	false	The total number of (interval) inv580_sent.	true
INV580_RCVD	COUNTER	false	The total number of (interval) inv580_rcvd.	true
INV602_SENT	COUNTER	false	The total number of (interval) inv602_sent.	true
INV602_RCVD	COUNTER	false	The total number of (interval) inv602_rcvd.	true
INV603_SENT	COUNTER	false	The total number of (interval) inv603_sent.	true
INV603_RCVD	COUNTER	false	The total number of (interval) inv603_rcvd.	true
INV606_SENT	COUNTER	false	The total number of (interval) inv606_sent.	true
INV606_RCVD	COUNTER	false	The total number of (interval) inv606_rcvd.	true
INVUNKNOWN_SENT	COUNTER	false	The total number of (interval) invUnknown_sent.	true
INVUNKNOWN_RCVD	COUNTER	false	The total number of (interval) invUnknown_rcvd.	true
NON_INV200_SENT	COUNTER	false	The total number of (interval) nonInv200_sent.	true
NON_INV200_RCVD	COUNTER	false	The total number of (interval) nonInv200_rcvd.	true
NON_INV380_SENT	COUNTER	false	The total number of (interval) nonInv380_sent.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INV380_RCVD	COUNTER	false	The total number of (interval) nonInv380_rcvd.	true
NON_INV400_SENT	COUNTER	false	The total number of (interval) nonInv400_sent.	true
NON_INV400_RCVD	COUNTER	false	The total number of (interval) nonInv400_rcvd.	true
NON_INV403_SENT	COUNTER	false	The total number of (interval) nonInv403_sent.	true
NON_INV403_RCVD	COUNTER	false	The total number of (interval) nonInv403_rcvd.	true
NON_INV404_SENT	COUNTER	false	The total number of (interval) nonInv404_sent.	true
NON_INV404_RCVD	COUNTER	false	The total number of (interval) nonInv404_rcvd.	true
NON_INV406_SENT	COUNTER	false	The total number of (interval) nonInv406_sent.	true
NON_INV406_RCVD	COUNTER	false	The total number of (interval) nonInv406_rcvd.	true
NON_INV408_SENT	COUNTER	false	The total number of (interval) nonInv408_sent.	true
NON_INV408_RCVD	COUNTER	false	The total number of (interval) nonInv408_rcvd.	true
NON_INV410_SENT	COUNTER	false	The total number of (interval) nonInv410_sent.	true
NON_INV410_RCVD	COUNTER	false	The total number of (interval) nonInv410_rcvd.	true
NON_INV420_SENT	COUNTER	false	The total number of (interval) nonInv420_sent.	true
NON_INV420_RCVD	COUNTER	false	The total number of (interval) nonInv420_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INV480_SENT	COUNTER	false	The total number of (interval) nonInv480_sent.	true
NON_INV480_RCVD	COUNTER	false	The total number of (interval) nonInv480_rcvd.	true
NON_INV481_SENT	COUNTER	false	The total number of (interval) nonInv481_sent.	true
NON_INV481_RCVD	COUNTER	false	The total number of (interval) nonInv481_rcvd.	true
NON_INV482_SENT	COUNTER	false	The total number of (interval) nonInv482_sent.	true
NON_INV482_RCVD	COUNTER	false	The total number of (interval) nonInv482_rcvd.	true
NON_INV483_SENT	COUNTER	false	The total number of (interval) nonInv483_sent.	true
NON_INV483_RCVD	COUNTER	false	The total number of (interval) nonInv483_rcvd.	true
NON_INV484_SENT	COUNTER	false	The total number of (interval) nonInv484_sent.	true
NON_INV484_RCVD	COUNTER	false	The total number of (interval) nonInv484_rcvd.	true
NON_INV486_SENT	COUNTER	false	The total number of (interval) nonInv486_sent.	true
NON_INV486_RCVD	COUNTER	false	The total number of (interval) nonInv486_rcvd.	true
NON_INV487_SENT	COUNTER	false	The total number of (interval) nonInv487_sent.	true
NON_INV487_RCVD	COUNTER	false	The total number of (interval) nonInv487_rcvd.	true
NON_INV488_SENT	COUNTER	false	The total number of (interval) nonInv488_sent.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INV488_RCVD	COUNTER	false	The total number of (interval) nonInv488_rcvd.	true
NON_INV500_SENT	COUNTER	false	The total number of (interval) nonInv500_sent.	true
NON_INV500_RCVD	COUNTER	false	The total number of (interval) nonInv500_rcvd.	true
NON_INV501_SENT	COUNTER	false	The total number of (interval) nonInv501_sent.	true
NON_INV501_RCVD	COUNTER	false	The total number of (interval) nonInv501_rcvd.	true
NON_INV502_SENT	COUNTER	false	The total number of (interval) nonInv502_sent.	true
NON_INV502_RCVD	COUNTER	false	The total number of (interval) nonInv502_rcvd.	true
NON_INV503_SENT	COUNTER	false	The total number of (interval) nonInv503_sent.	true
NON_INV503_RCVD	COUNTER	false	The total number of (interval) nonInv503_rcvd.	true
NON_INV504_SENT	COUNTER	false	The total number of (interval) nonInv504_sent.	true
NON_INV504_RCVD	COUNTER	false	The total number of (interval) nonInv504_rcvd.	true
NON_INV580_SENT	COUNTER	false	The total number of (interval) nonInv580_sent.	true
NON_INV580_RCVD	COUNTER	false	The total number of (interval) nonInv580_rcvd.	true
NON_INV602_SENT	COUNTER	false	The total number of (interval) nonInv602_sent.	true
NON_INV602_RCVD	COUNTER	false	The total number of (interval) nonInv602_rcvd.	true

Column Name	Column Type	Index	Description	canAggregate
NON_INV603_SENT	COUNTER	false	The total number of (interval) nonInv603_sent.	true
NON_INV603_RCVD	COUNTER	false	The total number of (interval) nonInv603_rcvd.	true
NON_INV606_SENT	COUNTER	false	The total number of (interval) nonInv606_sent.	true
INV606_RCVD	COUNTER	false	The total number of (interval) nonInv606_rcvd.	true
NON_INVUNKNOWN_SENT	COUNTER	false	The total number of (interval) nonInvUnknown_sent.	true
NON_INVUNKNOWN_RCVD	COUNTER	false	The total number of (interval) nonInvUnknown_rcvd.	true
CE_NAME	STRING	false	The name of the compute element for this entry.	False

SBCCORESipTgCSSRIntStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
ACNAME	STRING	true	The name of the address context.	false	N/A
ZNAME	STRING	true	The name of the address context zone.	false	N/A
NAME	STRING	true	The name of this SIP trunk group.	false	N/A
SUM_INV_SENT	COUNTER	false	The total number of (interval) inv_sent.	true	SUM
SUM_INV_RCVD	COUNTER	false	The total number of (interval) inv_rcvd.	true	SUM
SUM_ALERT_SENT	COUNTER	false	The total number of (interval) 18x_sent.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_ALERT_RC VD	COUNTER	false	The total number of (interval) 18x_rcvd.	true	SUM
SUM_ANSCALLS _SENT	COUNTER	false	The total number of (interval) ansCalls_sent.	true	SUM
SUM_ANSCALLS _RCVD	COUNTER	false	The total number of (interval) ansCalls_rcvd.	true	SUM
SUM_CANCEL_S ENT	COUNTER	false	The total number of (interval) cancel_sent.	true	SUM
SUM_CANCEL_R CVD	COUNTER	false	The total number of (interval) cancel_rcvd.	true	SUM
SUM_BYE_SENT	COUNTER	false	The total number of (interval) bye_sent.	true	SUM
SUM_BYE_RCVD	COUNTER	false	The total number of (interval) bye_rcvd.	true	SUM
SUM_INV200_SE NT	COUNTER	false	The total number of (interval) inv200_sent.	true	SUM
SUM_INV200_RC VD	COUNTER	false	The total number of (interval) inv200_rcvd.	true	SUM
SUM_INV380_SE NT	COUNTER	false	The total number of (interval) inv380_sent.	true	SUM
SUM_INV380_RC VD	COUNTER	false	The total number of (interval) inv380_rcvd.	true	SUM
SUM_INV400_SE NT	COUNTER	false	The total number of (interval) inv400_sent.	true	SUM
SUM_INV400_RC VD	COUNTER	false	The total number of (interval) inv400_rcvd.	true	SUM
SUM_INV403_SE NT	COUNTER	false	The total number of (interval) inv403_sent.	true	SUM
SUM_INV403_RC VD	COUNTER	false	The total number of (interval) inv403_rcvd.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_INV404_SENT	COUNTER	false	The total number of (interval) inv404_sent.	true	SUM
SUM_INV404_RCVD	COUNTER	false	The total number of (interval) inv404_rcvd.	true	SUM
SUM_INV406_SENT	COUNTER	false	The total number of (interval) inv406_sent.	true	SUM
SUM_INV406_RCVD	COUNTER	false	The total number of (interval) inv406_rcvd.	true	SUM
SUM_INV408_SENT	COUNTER	false	The total number of (interval) inv408_sent.	true	SUM
SUM_INV408_RCVD	COUNTER	false	The total number of (interval) inv408_rcvd.	true	SUM
SUM_INV410_SENT	COUNTER	false	The total number of (interval) inv410_sent.	true	SUM
SUM_INV410_RCVD	COUNTER	false	The total number of (interval) inv410_rcvd.	true	SUM
SUM_INV420_SENT	COUNTER	false	The total number of (interval) inv420_sent.	true	SUM
SUM_INV420_RCVD	COUNTER	false	The total number of (interval) inv420_rcvd.	true	SUM
SUM_INV480_SENT	COUNTER	false	The total number of (interval) inv480_sent.	true	SUM
SUM_INV480_RCVD	COUNTER	false	The total number of (interval) inv480_rcvd.	true	SUM
SUM_INV481_SENT	COUNTER	false	The total number of (interval) inv481_sent.	true	SUM
SUM_INV481_RCVD	COUNTER	false	The total number of (interval) inv481_rcvd.	true	SUM
SUM_INV482_SENT	COUNTER	false	The total number of (interval) inv482_sent.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_INV482_RC VD	COUNTER	false	The total number of (interval) inv482_rcvd.	true	SUM
SUM_INV483_SE NT	COUNTER	false	The total number of (interval) inv483_sent.	true	SUM
SUM_INV483_RC VD	COUNTER	false	The total number of (interval) inv483_rcvd.	true	SUM
SUM_INV484_SE NT	COUNTER	false	The total number of (interval) inv484_sent.	true	SUM
SUM_INV484_RC VD	COUNTER	false	The total number of (interval) inv484_rcvd.	true	SUM
SUM_INV486_SE NT	COUNTER	false	The total number of (interval) inv486_sent.	true	SUM
SUM_INV486_RC VD	COUNTER	false	The total number of (interval) inv486_rcvd.	true	SUM
SUM_INV487_SE NT	COUNTER	false	The total number of (interval) inv487_sent.	true	SUM
SUM_INV487_RC VD	COUNTER	false	The total number of (interval) inv487_rcvd.	true	SUM
SUM_INV488_SE NT	COUNTER	false	The total number of (interval) inv488_sent.	true	SUM
SUM_INV488_RC VD	COUNTER	false	The total number of (interval) inv488_rcvd.	true	SUM
SUM_INV500_SE NT	COUNTER	false	The total number of (interval) inv500_sent.	true	SUM
SUM_INV500_RC VD	COUNTER	false	The total number of (interval) inv500_rcvd.	true	SUM
SUM_INV501_SE NT	COUNTER	false	The total number of (interval) inv501_sent.	true	SUM
SUM_INV501_RC VD	COUNTER	false	The total number of (interval) inv501_rcvd.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_INV502_SENT	COUNTER	false	The total number of (interval) inv502_sent.	true	SUM
SUM_INV502_RCVD	COUNTER	false	The total number of (interval) inv502_rcvd.	true	SUM
SUM_INV503_SENT	COUNTER	false	The total number of (interval) inv503_sent.	true	SUM
SUM_INV503_RCVD	COUNTER	false	The total number of (interval) inv503_rcvd.	true	SUM
SUM_INV504_SENT	COUNTER	false	The total number of (interval) inv504_sent.	true	SUM
SUM_INV504_RCVD	COUNTER	false	The total number of (interval) inv504_rcvd.	true	SUM
SUM_INV580_SENT	COUNTER	false	The total number of (interval) inv580_sent.	true	SUM
SUM_INV580_RCVD	COUNTER	false	The total number of (interval) inv580_rcvd.	true	SUM
SUM_INV602_SENT	COUNTER	false	The total number of (interval) inv602_sent.	true	SUM
SUM_INV602_RCVD	COUNTER	false	The total number of (interval) inv602_rcvd.	true	SUM
SUM_INV603_SENT	COUNTER	false	The total number of (interval) inv603_sent.	true	SUM
SUM_INV603_RCVD	COUNTER	false	The total number of (interval) inv603_rcvd.	true	SUM
SUM_INV606_SENT	COUNTER	false	The total number of (interval) inv606_sent.	true	SUM
SUM_INV606_RCVD	COUNTER	false	The total number of (interval) inv606_rcvd.	true	SUM
SUM_INVUNKNO WN_SENT	COUNTER	false	The total number of (interval) invUnknown_sent.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_INVUNKNO WN_RCVD	COUNTER	false	The total number of (interval) invUnknown_rcvd.	true	SUM
SUM_NON_INV20 0_SENT	COUNTER	false	The total number of (interval) nonInv200_sent.	true	SUM
SUM_NON_INV20 0_RCVD	COUNTER	false	The total number of (interval) nonInv200_sent.	true	SUM
SUM_NON_INV38 0_SENT	COUNTER	false	The total number of (interval) nonInv380_sent.	true	SUM
SUM_NON_INV38 0_RCVD	COUNTER	false	The total number of (interval) nonInv380_rcvd.	true	SUM
SUM_NON_INV40 0_SENT	COUNTER	false	The total number of (interval) nonInv400_sent.	true	SUM
SUM_NON_INV40 0_RCVD	COUNTER	false	The total number of (interval) nonInv400_rcvd.	true	SUM
SUM_NON_INV40 3_SENT	COUNTER	false	The total number of (interval) nonInv403_sent.	true	SUM
SUM_NON_INV40 3_RCVD	COUNTER	false	The total number of (interval) nonInv403_rcvd.	true	SUM
SUM_NON_INV40 4_SENT	COUNTER	false	The total number of (interval) nonInv404_sent.	true	SUM
SUM_NON_INV40 4_RCVD	COUNTER	false	The total number of (interval) nonInv404_rcvd.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_NON_INV406_SENT	COUNTER	false	The total number of (interval) nonInv406_sent.	true	SUM
SUM_NON_INV406_RCVD	COUNTER	false	The total number of (interval) nonInv406_rcvd.	true	SUM
SUM_NON_INV408_SENT	COUNTER	false	The total number of (interval) nonInv408_sent.	true	SUM
SUM_NON_INV408_RCVD	COUNTER	false	The total number of (interval) nonInv408_rcvd.	true	SUM
SUM_NON_INV410_SENT	COUNTER	false	The total number of (interval) nonInv410_sent.	true	SUM
SUM_NON_INV410_RCVD	COUNTER	false	The total number of (interval) nonInv410_rcvd.	true	SUM
SUM_NON_INV420_SENT	COUNTER	false	The total number of (interval) nonInv420_sent.	true	SUM
SUM_NON_INV420_RCVD	COUNTER	false	The total number of (interval) nonInv420_rcvd.	true	SUM
SUM_NON_INV480_SENT	COUNTER	false	The total number of (interval) nonInv480_sent.	true	SUM
SUM_NON_INV480_RCVD	COUNTER	false	The total number of (interval) nonInv480_rcvd.	true	SUM
SUM_NON_INV481_SENT	COUNTER	false	The total number of (interval) nonInv481_sent.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_NON_INV48 1_RCVD	COUNTER	false	The total number of (interval) nonInv481_rcvd.	true	SUM
SUM_NON_INV48 2_SENT	COUNTER	false	The total number of (interval) nonInv482_sent.	true	SUM
SUM_NON_INV48 2_RCVD	COUNTER	false	The total number of (interval) nonInv482_rcvd.	true	SUM
SUM_NON_INV48 3_SENT	COUNTER	false	The total number of (interval) nonInv483_sent.	true	SUM
SUM_NON_INV48 3_RCVD	COUNTER	false	The total number of (interval) nonInv483_rcvd.	true	SUM
SUM_NON_INV48 4_SENT	COUNTER	false	The total number of (interval) nonInv484_sent.	true	SUM
SUM_NON_INV48 4_RCVD	COUNTER	false	The total number of (interval) nonInv484_rcvd.	true	SUM
SUM_NON_INV48 6_SENT	COUNTER	false	The total number of (interval) nonInv486_sent.	true	SUM
SUM_NON_INV48 6_RCVD	COUNTER	false	The total number of (interval) nonInv486_rcvd.	true	SUM
SUM_NON_INV48 7_SENT	COUNTER	false	The total number of (interval) nonInv487_sent.	true	SUM
SUM_NON_INV48 7_RCVD	COUNTER	false	The total number of (interval) nonInv487_rcvd.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_NON_INV488_SENT	COUNTER	false	The total number of (interval) nonInv488_sent.	true	SUM
SUM_NON_INV488_RCVD	COUNTER	false	The total number of (interval) nonInv488_rcvd.	true	SUM
SUM_NON_INV500_SENT	COUNTER	false	The total number of (interval) nonInv500_sent.	true	SUM
SUM_NON_INV500_RCVD	COUNTER	false	The total number of (interval) nonInv500_rcvd.	true	SUM
SUM_NON_INV501_SENT	COUNTER	false	The total number of (interval) nonInv501_sent.	true	SUM
SUM_NON_INV501_RCVD	COUNTER	false	The total number of (interval) nonInv501_rcvd.	true	SUM
SUM_NON_INV502_SENT	COUNTER	false	The total number of (interval) nonInv502_sent.	true	SUM
SUM_NON_INV502_RCVD	COUNTER	false	The total number of (interval) nonInv502_rcvd.	true	SUM
SUM_NON_INV503_SENT	COUNTER	false	The total number of (interval) nonInv503_sent.	true	SUM
SUM_NON_INV503_RCVD	COUNTER	false	The total number of (interval) nonInv503_rcvd.	true	SUM
SUM_NON_INV504_SENT	COUNTER	false	The total number of (interval) nonInv504_sent.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
SUM_NON_INV504_RCVD	COUNTER	false	The total number of (interval) nonInv504_rcvd.	true	SUM
SUM_NON_INV580_SENT	COUNTER	false	The total number of (interval) nonInv580_sent.	true	SUM
SUM_NON_INV580_RCVD	COUNTER	false	The total number of (interval) nonInv580_rcvd.	true	SUM
SUM_NON_INV602_SENT	COUNTER	false	The total number of (interval) nonInv602_sent.	true	SUM
SUM_NON_INV602_RCVD	COUNTER	false	The total number of (interval) nonInv602_rcvd.	true	SUM
SUM_NON_INV603_SENT	COUNTER	false	The total number of (interval) nonInv603_sent.	true	SUM
SUM_NON_INV603_RCVD	COUNTER	false	The total number of (interval) nonInv603_rcvd.	true	SUM
SUM_SUM_NON_INV606_SENT	COUNTER	false	The total number of (interval) nonInv606_sent.	true	SUM
SUM_INV606_RCVD	COUNTER	false	The total number of (interval) nonInv606_rcvd.	true	SUM
SUM_NON_INVU_NKNOWN_SENT	COUNTER	false	The total number of (interval) nonInvUnknown_sent.	true	SUM
SUM_NON_INVU_NKNOWN_RCVD	COUNTER	false	The total number of (interval) nonInvUnknown_rcvd.	true	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregation Type
CE_NAME	STRING	false	The name of the compute element for this entry.	false	N/A

SBCCORESipTGRResIntStats

Column name	Column type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	True	The name of this address context.	False	N/A
ZNAME	STRING	True	The name of the address context zone.	False	N/A
NAME	STRING	True	The name of this SIP trunk group.	False	N/A
DIRECTION	STRING	True	The direction of (Interval) SIP response messages.	False	N/A
RESPONSE_CODE	INTEGER	True	The response code of (Interval) SIP response messages.	False	N/A
RESPONSE_COUNT	INTEGER	False	The total number of (Interval) SIP response messages for the specified response code.	True	AVG
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBCCORESipTGRResIntStats_AG

Column name	Column type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	True	The name of this Address Context.	False	N/A
ZNAME	STRING	True	The name of the address context zone.	False	N/A
NAME	STRING	True	The name of this SIP trunk group.	False	N/A

Column name	Column type	Index	Description	canAggregate	Aggregate Type
DIRECTION	STRING	True	The direction of (Interval) SIP response messages.	False	N/A
RESPONSE_CODE	INTEGER	True	The response code of (Interval) SIP response messages.	False	N/A
RESPONSE_COUNT	INTEGER	False	The total number of (Interval) SIP response messages for the specified response code.	True	AVG
CE_NAME	STRING	False	The name of the compute element for this entry.	False	N/A

SBX5KSipByeResponseIntervalStats

Name	Type	Index	Description	canAggregate
ACNAME	STRING	True	The name of the address context.	False
ZNAME	STRING	True	The name of the address context zone.	False
NAME	STRING	True	The name of this SIP peer group.	False
BYE_RESPONSE_401	COUNTER	False	Indicates the total number of (interval) 401 responses for received Bye messages.	True
BYE_RESPONSE_403	COUNTER	False	Indicates the total number of (interval) 403 responses for received Bye messages.	True
BYE_RESPONSE_407	COUNTER	False	Indicates the total number of (interval) 407 responses for received Bye messages.	True
BYE_RESPONSE_481	COUNTER	False	Indicates the total number of (interval) 481 responses for received Bye messages.	True
CE_NAME	STRING	False	The name of the compute element for this entry.	False

SBX5KSipInviteResponseIntervalStats

Name	Index	Type	Description	CanAggregate
ACNAME	True	STRING	The name of the address context.	False
ZNAME	True	STRING	The name of the address context zone.	False
NAME	True	STRING	The name of this SIP peer group.	False
INV_RESPONSE_401	False	COUNTER	Indicates the total number of (interval) 401 responses for received Invite messages.	True
INV_RESPONSE_403	False	COUNTER	Indicates the total number of (interval) 403 responses for received Invite messages.	True
INV_RESPONSE_407	False	COUNTER	Indicates the total number of (interval) 407 responses for received Invite messages.	True
INV_RESPONSE_481	False	COUNTER	Indicates the total number of (interval) 481 responses for received Invite messages.	True
CE_NAME	False	STRING	The name of the compute element for this entry.	False

SBX5KSipRegResponseIntervalStats

Name	Index	Type	Description	canAggregate
ACNAME	True	STRING	The name of the address context.	False
ZNAME	True	STRING	The name of the address context zone.	False
NAME	True	STRING	The name of this SIP peer group.	False
REG_RESPONSE_401	False	COUNTER	Indicates the total number of (interval) 401 responses for received Register messages.	True

Name	Index	Type	Description	canAggregate
REG_RESPONSE_403	False	COUNTER	Indicates the total number of (interval) 403 responses for received Register messages.	True
REG_RESPONSE_407	False	COUNTER	Indicates the total number of (interval) 407 responses for received Register messages.	True
REG_RESPONSE_481	False	COUNTER	Indicates the total number of (interval) 481 responses for received Register messages.	True
CE_NAME	False	STRING	The name of the compute element for this entry.	False

SBX5KSystemDspStatusDspUsageStats

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
SYSTEM_NAME	STRING	True	Name of the system.		Show Status System
COMPRESSION_TOTAL	INTEGER	False	Total compression resource capacity on this server.		
COMPRESSION_UTILIZATION	INTEGER	False	Percentage utilization of compression resources on this server.		
COMPRESSION_ALLOC_FAILURES	INTEGER	False	Percentage of compression resources allocation failures on this server.		
G711_TOTAL	INTEGER	False	Total G711 resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711_UTILIZATION	INTEGER	False	Percentage utilization of G711 resources on this server.		
G726_TOTAL	INTEGER	False	Total G726 resource capacity on this server.		
G726_UTILIZATION	INTEGER	False	Percentage utilization of G726 resources on this server.		
G729AB_TOTAL	INTEGER	False	Total G729A+B resource capacity on this server.		
G729AB_UTILIZATION	INTEGER	False	Percentage utilization of G729A+B resources on this server.		
G7231_TOTAL	INTEGER	False	Total G723.1 resource capacity on this server.		
G7231_UTILIZATION	INTEGER	False	Percentage utilization of G7231 resources on this server.		
ILBC_TOTAL	INTEGER	False	Total iLBC resource capacity on this server.		
ILBC_UTILIZATION	INTEGER	False	Percentage utilization of iLBC resources on this server.		
ILBC_ALLOC_FAILURES	INTEGER	False	Percentage of iLBC resources allocation failures on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
ECM_TOTAL	INTEGER	False	Total T.38 ECM resource capacity on this server.		
ECM_UTILIZATION	INTEGER	False	Percentage utilization of T.38 ECM resources on this server.		
ECM_ALLOC_FAILURES	INTEGER	False	Percentage of T.38 ECM resources allocation failures on this server.		
TONE_TOTAL	INTEGER	False	Total tone resource capacity on this server.		
TONE_UTILIZATION	INTEGER	False	Percentage utilization of tone resources on this server.		
TONE_ALLOC_FAILURES	INTEGER	False	Percentage of tone resource allocation failures on this server.		
EVRCB0_TOTAL	INTEGER	False	Total EVRCB0 resource capacity on this server.		
EVRCB0_UTILIZATION	INTEGER	False	Percentage utilization of EVRCB0 resources on this server.		
EVRCB0_ALLOC_FAILURES	INTEGER	False	Percentage of EVRCB0 resources allocation failures on this server.		
AMRNB_TOTAL	INTEGER	False	Total AMR-NB resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
AMRNB_UTILIZATION	INTEGER	False	Percentage utilization of AMR-NB resources on this server.		
AMRNB_ALLOC_FAILURES	INTEGER	False	Percentage of AMR-NB resources allocation failures on this server.		
AMRWB_TOTAL	INTEGER	False	Total AMR-WB resource capacity on this server.		
AMRWB_UTILIZATION	INTEGER	False	Percentage utilization of AMR-WB resources on this server.		
AMRWB_ALLOC_FAILURES	INTEGER	False	Percentage of AMR-WB resources allocation failures on this server.		
G722_TOTAL	INTEGER	False	Total G.722 resource capacity on this server.		
G722_UTILIZATION	INTEGER	False	Percentage utilization of G.722 resources on this server.		
G722_ALLOC_FAILURES	INTEGER	False	Percentage of G.722 resources allocation failures on this server.		
EVRC0_TOTAL	INTEGER	False	Total EVRC0 resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
EVRC0_UTILIZATION	INTEGER	False	Percentage utilization of EVRC0 resources on this server.		
EVRC0_ALLOC_FAILURES	INTEGER	False	Percentage of EVRC0 resources allocation failures on this server.		
COMPRESSION_AVAILABLE	INTEGER	False	Number of compression resources currently unused and available on this server.		
TONE_AVAILABLE	INTEGER	False	Number of tone resources currently unused and available on this server.		
G7221_TOTAL	INTEGER	False	Total G.722.1 resource capacity on this server.		
G7221_UTILIZATION	INTEGER	False	Percentage utilization of G.722.1 resources on this server.		
EFR_TOTAL	INTEGER	False	Total EFR resource capacity on this server.		
EFR_UTILIZATION	INTEGER	False	Percentage utilization of EFR resources on this server.		
G711SS_TOTAL	INTEGER	False	Total G711SS (silence suppression) resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SS_UTILIZATION	INTEGER	False	Percentage utilization of G711SS (silence suppression) resources on this server.		
SLOT1_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
SLOT2_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
SLOT3_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
SLOT4_RESOURCES_UTILIZED	INTEGER	False	Total compression/ tone resources in use on this module slot.		
G711V8_TOTAL	INTEGER	False	Total G711 V8 resource capacity on this server.		
G711V8_UTILIZATION	INTEGER	False	Percentage utilization of G711 V8 resources on this server.		
G711SSV8_TOTAL	INTEGER	False	Total G711SS (silence suppression) V8 resource capacity on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SSV8_UTILIZATION	INTEGER	False	Percentage utilization of G711SS (silence suppression) V8 resources on this server.		
G726V8_TOTAL	INTEGER	False	Total G726 V8 resource capacity on this server.		
G726V8_UTILIZATION	INTEGER	False	Percentage utilization of G726 V8 resources on this server.		
G7231V8_TOTAL	INTEGER	False	Total G723.1 V8 resource capacity on this server.		
G7231V8_UTILIZATION	INTEGER	False	Percentage utilization of G7231 V8 resources on this server.		
G722V8_TOTAL	INTEGER	False	Total G.722 V8 resource capacity on this server.		
G722V8_UTILIZATION	INTEGER	False	Percentage utilization of G.722 V8 resources on this server.		
G7221V8_TOTAL	INTEGER	False	Total G.722.1 V8 resource capacity on this server.		
G7221V8_UTILIZATION	INTEGER	False	Percentage utilization of G.722.1 V8 resources on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G729ABV8_TOTAL	INTEGER	False	Total G729A+B V8 resource capacity on this server.		
G729ABV8_UTILIZATION	INTEGER	False	Percentage utilization of G729A+B V8 resources on this server.		
ECMV34_TOTAL	INTEGER	False	Total T.38 ECM V.34 resource capacity on this server.		
ECMV34_UTILIZATION	INTEGER	False	Percentage utilization of T.38 ECM V.34 resources on this server.		
ILBCV8_TOTAL	INTEGER	False	Total iLBC V8 resource capacity on this server.		
ILBCV8_UTILIZATION	INTEGER	False	Percentage utilization of iLBC V8 resources on this server.		
OPUS_TOTAL	INTEGER	False	Total OPUS resource capacity on this server.		
OPUS_UTILIZATION	INTEGER	False	Percentage utilization of OPUS resources on this server.		
OPUS_ALLOC_FAILURES	INTEGER	False	Percentage of OPUS resources allocation failures on this server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
USAGE_EVS_TOTAL	INTEGER	False	The total EVS resource capacity on this server.		
USAGE_EVS_UTILIZATION	INTEGER	False	The percentage utilization of EVS resources on this server.		
USAGE_SILK_8_TOTAL	COUNT	False	Total SILK_8 resource capacity on the present server		
USAGE_SILK_8_UTILIZATION	COUNT	False	Percentage utilization of SILK_8 resources on the present server		
USAGE_SILK_16_TOTAL	COUNT	False	Total SILK_16 resource capacity on the present server		
USAGE_SILK_16_UTILIZATION	COUNT	False	Percentage utilization of SILK_16 resources on the present server		
USAGE_AMR_NBT140_TOTAL	INTEGER	True	Total AMR-NB with T.140 resource capacity in the server.		
USAGE_AMR_NBT140_UTILIZATION	INTEGER	False	The utilization percentage of AMR-NB with T.140 resource in the server.		
USAGE_AMR_WBT140_TOTAL	INTEGER	False	Total AMR-WB with T.140 resource capacity in the server.		

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
USAGE_AMR_WBT140_UTILIZATION	INTEGER	False	The utilization percentage of AMR-WB with T.140 resource in the server.		
COMP_HP_UTILIZATION	INTEGER	False	Percentage utilization of AMR-WB with T.140 resource on this server.		
RESOURCE_HP_UTILIZATION	INTEGER	False	Percentage utilization of tone resources used for high priority calls on this server.		
DSP_EVS_T140_TOTAL	INTEGER	False	Total EVS with T.140 resource capacity on this server.		
DSP_EVS_T140_UTILIZATION	INTEGER	False	Percentage utilization of EVS with T.140 resources on this server		
G711T140_TOTAL	GAUGE	False	The total G711 with T.140 resource capacity on this server.	MEAN	
G711T140_UTILIZATION	GAUGE	False	The percentage utilization of G711 with T.140 resources on this server.	MEAN	
G711SST140_TOTAL	GAUGE	False	The total G711SS with T.140 resource capacity on this server.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711SST140_UTILIZATION	GAUGE	False	The percentage utilization of G711SS with T.140 resources on this server.	MEAN	
OPUST140_TOTAL	GAUGE	False	The total Opus with T.140 resource capacity on this server.	MEAN	
OPUST140_UTILIZATION	GAUGE	False	The percentage utilization of Opus with T.140 resources on this server.	MEAN	
G722T140_TOTAL	GAUGE	False	The total G722 with T.140 resource capacity on this server.	MEAN	
G722T140_UTILIZATION	GAUGE	False	The percentage utilization of G722 with T.140 resources on this server.	MEAN	
G722V8T140_TOTAL	GAUGE	False	The total G722 V8 with T.140 resource capacity on this server.	MEAN	
G722V8T140_UTILIZATION	GAUGE	False	The percentage utilization of G722 V8 with T.140 resources on this server.	MEAN	
G711V8T140_TOTAL	GAUGE	False	The total G711 V8 with T.140 resource capacity on this server.	MEAN	

Column Name	Column Type	Index	Description	Aggregate Type	CLI Command Reference
G711V8T140_UTILIZATION	GAUGE	False	The percentage utilization of G711 V8 with T.140 resources on this server.	MEAN	
G711SSV8T140_TOTAL	GAUGE	False	The total G711SS V8 with T.140 resource capacity on this server.	MEAN	
G711SSV8T140_UTILIZATION	GAUGE	False	The percentage utilization of G711SS V8 with T.140 resources on this server.	MEAN	
L16_TOTAL	GAUGE	False	The total L16 resource capacity on this server.	MEAN	
L16_UTILIZATION	GAUGE	False	The percentage utilization of L16 resources on this server.	MEAN	
CE_NAME	STRING	False	The name of the compute element for this entry.	N/A	

SipIntervalStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ZNAME	STRING	Yes	The name of the address context zone.	False	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
NAME	STRING	Yes	The name of this SIP trunk group.	True	
RCV_INVITE	COUNTER	No	Indicates the total number of (interval) received Invite messages.	False	
SND_INVITE	COUNTER	No	Indicates the total number of (interval) sent Invite messages.	True	
RCV_ACK	COUNTER	No	Indicates the total number of (interval) Received Ack.	True	
SND_ACK	COUNTER	No	Indicates the total number of (interval) Sent Ack messages.	True	
RCV_PRACK	COUNTER	No	Indicates the total number of (interval) received Prack messages.	True	
SND_PRACK	COUNTER	No	Indicates the total number of (interval) sent Prack messages.	True	
RCV_INFO	COUNTER	No	Indicates the total number of (interval) received INFO messages.	True	
SND_INFO	COUNTER	No	Indicates the total number of (interval) sent INFO messages.	True	
RCV_REFERER	COUNTER	No	Indicates the total number of (interval) received Refer messages.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SND_REFER	COUNTER	No	Indicates the total number of (interval) sent Refer messages.	True	
RCV_BYE	COUNTER	No	Indicates the total number of (interval) Received Bye messages.	True	
SND_BYE	COUNTER	No	Indicates the total number of (interval) sent Bye messages.	True	
RCV_CANCEL	COUNTER	No	Indicates the total number of (interval) received Cancel messages.	True	
SND_CANCEL	COUNTER	No	Indicates the total number of (interval) sent Cancel messages.	True	
RCV_REGISTER	COUNTER	No	Indicates the total number of (interval) received Register messages.	True	
SND_REGISTER	COUNTER	No	Indicates the total number of (interval) sent Register messages.	True	
RCV_UPDATE	COUNTER	No	Indicates the total number of (interval) received Update messages.	True	
SND_UPDATE	COUNTER	No	Indicates the total number of (interval) sent Update messages.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
RCV18_X	COUNTER	No	Indicates the total number of (interval) received 18x messages.	True	
SND18_X	COUNTER	No	Indicates the total number of (interval) sent 18x messages.	True	
RCV1_XX	COUNTER	No	Indicates the total number of (interval) received 1xx messages except 18x messages.	True	
SND1_XX	COUNTER	No	Indicates the total number of (interval) sent 1xx messages except 18x messages.	True	
RCV2_XX	COUNTER	No	Indicates the total number of (interval) received 2xx (Invite) messages.	True	
SND2_XX	COUNTER	No	Indicates the total number of (interval) sent 2xx (Invite) messages.	True	
RCV_NON_I NV2_XX	COUNTER	No	Indicates the total number of (interval) received 2xx (Non-Invite) messages.	True	
SND_NON_I NV2_XX	COUNTER	No	Indicates the total number of (interval) sent 2xx (Non-Invite) messages.	True	
RCV3_XX	COUNTER	No	Indicates the total number of (interval) received 3xx messages.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
SND3_XX	COUNTER	No	Indicates the total number of (interval) sent 3xx messages.	True	
RCV4_XX	COUNTER	No	Indicates the total number of (interval) received 4xx messages.	True	
SND4_XX	COUNTER	No	Indicates the total number of (interval) sent 4xx messages.	True	
RCV5_XX	COUNTER	No	Indicates the total number of (interval) receive 5xx messages.	True	
SND5_XX	COUNTER	No	Indicates the total number of (interval) sent 5xx messages.	True	
RCV6_XX	COUNTER	No	Indicates the total number of (interval) receive 6xx messages.	True	
SND6_XX	COUNTER	No	Indicates the total number of (interval) sent 6xx messages.	True	
RCV_NON_INV_ERR	COUNTER	No	Indicates the total number of (interval) receive Nonlvite Error messages.	True	
SND_NON_INV_ERR	COUNTER	No	Indicates the total number of (interval) sent Nonlvite Error messages.	True	
RCV_UNKNOWN_MSG	COUNTER	No	Indicates the total number of (interval) receive Unknown messages.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
RCV_SUBSC RIBER	COUNTER	No	Indicates the total number of (interval) receive Subscriber messages.	True	
SNL_SUBSC RIBER	COUNTER	No	Indicates the total number of (interval) sent Subscriber messages.	True	
RCV_NOTIF Y	COUNTER	No	Indicates the total number of (interval) receive Notify messages.	True	
SNL_NOTIF Y	COUNTER	No	Indicates the total number of (interval) sent Notify messages.	True	
RCV_OPTIO N	COUNTER	No	Indicates the total number of (interval) receive Option messages.	True	
SNL_OPTIO N	COUNTER	No	Indicates the total number of (interval) sent Option messages.	True	
INV_RE_TRA NSMIT	COUNTER	No	Indicates the total number of (interval) Invite messages Re-Transmitted.	True	
REG_RE_TR ANSMIT	COUNTER	No	Indicates the total number of (interval) Register messages Re-Transmitted.	True	
BYE_RETRA NSMIT	COUNTER	No	Indicates the total number of (interval) Bye messages Re-Transmitted.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
CANCLE_RE_TRANSMIT	COUNTER	No	Indicates the total number of (interval) Cancel messages Re-Transmitted.	True	
OTHER_RE_TRANSMIT	COUNTER	No	Indicates the total number of (interval) Other messages Re-Transmitted.	True	
RCV_MESSAGE	COUNTER	No	Indicates the total number of (interval) received Message method.	True	
SEND_MESSAGE	COUNTER	No	Indicates the total number of (interval) sent Message method.	True	
RCV_PUBLISH	COUNTER	No	Indicates the total number of (interval) received Publish method.	True	
SEND_PUBLISH	COUNTER	No	Indicates the total number of (interval) sent Publish method.	True	
EMERGENCY_ACCEPT	COUNTER	No	Indicates the total number of (interval) emergency calls accepted.	True	
EMERGENCY_REJECT_BWCALL	COUNTER	No	Indicates the total number of (interval) emergency calls rejected because of bandwidth limit or call limit.	True	
EMERGENCY_REJECT_POLICER	COUNTER	No	Indicates the total number of (interval) emergency calls rejected because of Priority Policer.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
HPC_ACCEPT	COUNTER	No	Indicates the total number of (interval) HPC calls accepted.	True	
NUM_OF_CALLS_SENDING_AARS	COUNTER	No	Indicates the number of calls sending AAR requests.	True	
NUM_OF_RECEIVED_AAA_FAILURES	COUNTER	No	Indicates the number of received AAA failures.	True	
NUM_OF_RECEIVED_AAA_SUCCESSES	COUNTER	No	Indicates the number of received AAA Successes.	True	
NUM_OF_TOTAL_AAR_SENT	COUNTER	No	Indicates the total number of AAR messages sent.	True	
NUM_OF_TIMEOUT_OR_ERROR_AAR	COUNTER	No	Indicates the number of AAR messages not answered.	True	
NUM_OF_RECEIVED_RARS	COUNTER	No	Indicates the number of RAR messages received.	True	
NUM_OF_RECEIVED_ASRS	COUNTER	No	Indicates the number of ASR messages received.	True	
NUM_OF_SENT_STRS	COUNTER	No	Indicates the number of STR messages sent.	True	
EMERGENCY_REG_ACCEPT	COUNTER	No	Indicates the number of (interval) emergency registrations accepted.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
EMERGENCY_REG_REJECT_LIMIT	COUNTER	No	Indicates the number of (interval) emergency registrations rejected because of the registration limit.	True	
EMERGENCY_REG_REJECT_POLICER	COUNTER	No	Indicates the number of (interval) emergency registrations rejected because of the Priority Policer.	True	
EMERGENCY_OOD_ACCEPT	COUNTER	No	Indicates the number of (interval) emergency OOD Requests accepted.	True	
EMERGENCY_OOD_REJECT_POLICER	COUNTER	No	Indicates the number of (interval) emergency OOD Requests rejected because of the Priority Policer.	True	
EMERGENCY_SUBSCRIBE_ACCEPT	COUNTER	No	Indicates the number of (interval) emergency Subscribe Requests accepted.	True	
EMERGENCY_SUBS_REJECT_LIMIT	COUNTER	No	Indicates the number of (interval) emergency Subscribe Requests rejected because of the subscription limit.	True	
EMERGENCY_SUBS_REJECT_POLICER	COUNTER	No	Indicates the number of (interval) emergency Subscribe Requests rejected because of the Priority Policer.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
PARSE_ERROR	COUNTER	No	Indicates the total number of (interval) Parse Errors.	True	
NUM_OF_TOTAL_UDR_SENT	COUNTER	No	Indicates the total number of UDR messages sent.	True	
NUM_OF_TIMEOUT_UDR_ERROR	COUNTER	No	Indicates the number of UDR messages not answered.	True	
NUM_OF_RECEIVED_UDASUCCESS	COUNTER	No	Indicates the number of received UDA success	True	
NUM_OF_RECEIVED_UDAFAILURE	COUNTER	No	Indicates the number of received UDA failures.	True	
TOTAL_NUM_S8HR_OUT_REG	COUNTER	No	Indicates the total number (includes success and failed) of registration received from S8HR Outbound Roaming Users.	True	
NUM_S8HR_OUT_REG_SUCCESS	COUNTER	No	Indicates the number of successful registration from S8HR Outbound Roaming Users.	True	
NUM_S8HR_OUT_REG_FAILURE	COUNTER	No	Indicates the number of S8HR Outbound Roaming Users registrations failed.	True	
TOTAL_NUM_S8HR_OT_NML_CALL	COUNTER	No	Indicates the total number of normal calls initiated from S8HR Outbound Roaming Users.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
NUM_OF_S8 HR_OT_NML _CALL_SUC	COUNTER	No	Indicates the number of successful normal calls from S8HR Outbound Roaming Users.	True	
NUM_OF_S8 HR_OT_NML _CALL_FAIL	COUNTER	No	Indicates the total number of failed normal calls from S8HR Outbound Roaming Users.	True	
NUM_OF_S8 HR_OT_EMG _CALL_REJ	COUNTER	No	Indicates the number of S8HR Outbound Roaming User's emergency calls rejected.	True	
NUM_OF_S8 HR_IN_EMG _REG_SUC	COUNTER	No	Indicates the number of Successful registration from S8HR Inbound Roaming Users.	True	
NUM_OF_S8 HR_IN_EMG _REG_FAIL	COUNTER	No	Indicates the number of S8HR Inbound User's registration rejected.	True	
NUM_OF_S8 HR_IN_EMG _CALL_SUC	COUNTER	No	Indicates the number of successful emergency calls from S8HR Inbound User.	True	
NUM_OF_S8 HR_IN_EMG _CALL_FAIL	COUNTER	No	Indicates the number of S8HR Inbound Users emergency calls failed.	True	
NUM_OF_IN _HPC_CALL _ACC	INTEGER	No	Indicates the total number of (interval) Ingress HPC calls accepted.	True	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
NUM_OF_OUT_HPC_CALL_ACC	INTEGER	No	Indicates the total number of (interval) Engress HPC calls accepted.	True	
NUM_OF_HPC_4XX_MSG_SENT	INTEGER	No	Indicates the total number of (interval) sent HPC 4xx messages.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

SipIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
ZNAME	STRING	Yes	The name of the address context zone.	False	N/A
NAME	STRING	Yes	The name of this SIP trunk group.	False	N/A
SUM_RCV_INVITE	COUNTER	No	The sum of the total number of (interval) received Invite messages.	True	SUM
SUM_SND_INVITE	COUNTER	No	The sum of the total number of (interval) sent Invite messages.	True	SUM
SUM_RCV_ACK	COUNTER	No	The sum of the total number of (interval) Received Ack.	True	SUM
SUM_SND_ACK	COUNTER	No	The sum of the total number of (interval) Sent Ack messages.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_RCV_PRACK	COUNTER	No	The sum of the total number of (interval) received Prack messages.	True	SUM
SUM_SND_PRACK	COUNTER	No	The sum of the total number of (interval) sent Prack messages.	True	SUM
SUM_RCV_INFO	COUNTER	No	The sum of the total number of (interval) received INFO messages.	True	SUM
SUM_SND_INFO	COUNTER	No	The sum of the total number of (interval) sent INFO messages.	True	SUM
SUM_RCV_REFER	COUNTER	No	The sum of the total number of (interval) received Refer messages.	True	SUM
SUM_SND_REFER	COUNTER	No	The sum of the total number of (interval) sent Refer messages.	True	SUM
SUM_RCV_BYE	COUNTER	No	The sum of the total number of (interval) Received Bye messages.	True	SUM
SUM_SND_BYE	COUNTER	No	The sum of the total number of (interval) sent Bye messages.	True	SUM
SUM_RCV_CANCEL	COUNTER	No	The sum of the total number of (interval) received Cancel messages.	True	SUM
SUM_SND_CANCEL	COUNTER	No	The sum of the total number of (interval) sent Cancel messages.	True	SUM
SUM_RCV_REGISTER	COUNTER	No	The sum of the total number of (interval) received Register messages.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SND_REGISTER	COUNTER	No	The sum of the total number of (interval) sent Register messages.	True	SUM
SUM_RCV_UPDATE	COUNTER	No	The sum of the total number of (interval) received Update messages.	True	SUM
SUM_SND_UPDATE	COUNTER	No	The sum of the total number of (interval) sent Update messages.	True	SUM
SUM_RCV18_X	COUNTER	No	The sum of the total number of (interval) received 18x messages.	True	SUM
SUM_SND18_X	COUNTER	No	The sum of the total number of (interval) sent 18x messages.	True	SUM
SUM_RCV1_XX	COUNTER	No	The sum of the total number of (interval) received 1xx messages except 18x messages.	True	SUM
SUM_SND1_XX	COUNTER	No	The sum of the total number of (interval) sent 1xx messages except 18x messages.	True	SUM
SUM_RCV2_XX	COUNTER	No	The sum of the total number of (interval) received 2xx (Invite) messages.	True	SUM
SUM_SND2_XX	COUNTER	No	The sum of the total number of (interval) sent 2xx (Invite) messages.	True	SUM
SUM_RCV_NON_INV2_XX	COUNTER	No	The sum of the total number of (interval) received 2xx (Non-Invite) messages.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_SND_NON_I NV2_XX	COUNTER	No	The sum of the total number of (interval) sent 2xx (Non-Invite) messages.	True	SUM
SUM_RCV3_XX	COUNTER	No	The sum of the total number of (interval) received 3xx messages.	True	SUM
SUM_SND3_XX	COUNTER	No	The sum of the total number of (interval) sent 3xx messages.	True	SUM
SUM_RCV4_XX	COUNTER	No	The sum of the total number of (interval) received 4xx messages.	True	SUM
SUM_SND4_XX	COUNTER	No	The sum of the total number of (interval) sent 4xx messages.	True	SUM
SUM_RCV5_XX	COUNTER	No	The sum of the total number of (interval) receive 5xx messages.	True	SUM
SUM_SND5_XX	COUNTER	No	The sum of the total number of (interval) sent 5xx messages.	True	SUM
SUM_RCV6_XX	COUNTER	No	The sum of the total number of (interval) receive 6xx messages.	True	SUM
SUM_SND6_XX	COUNTER	No	The sum of the total number of (interval) sent 6xx messages.	True	SUM
SUM_RCV_NON_I NV_ERR	COUNTER	No	The sum of the total number of (interval) receive Nonlvite Error messages.	True	SUM
SUM_SND_NON_I NV_ERR	COUNTER	No	The sum of the total number of (interval) sent Nonlvite Error messages.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_RCV_UNKN OWN_MSG	COUNTER	No	The sum of the total number of (interval) receive Unknown messages.	True	SUM
SUM_RCV_SUBS CRIBER	COUNTER	No	The sum of the total number of (interval) receive Subscriber messages.	True	SUM
SUM_SND_SUBS CRIBER	COUNTER	No	The sum of the total number of (interval) sent Subscriber messages.	True	SUM
SUM_RCV_NOTIF Y	COUNTER	No	The sum of the total number of (interval) receive Notify messages.	True	SUM
SUM_SND_NOTIF Y	COUNTER	No	The sum of the total number of (interval) sent Notify messages.	True	SUM
SUM_RCV_OPTIO N	COUNTER	No	The sum of the total number of (interval) receive Option messages.	True	SUM
SUM_SND_OPTIO N	COUNTER	No	The sum of the total number of (interval) sent Option messages.	True	SUM
SUM_INV_RE_TR ANSMIT	COUNTER	No	The sum of the total number of (interval) Invite messages Re-Transmitted.	True	SUM
SUM_REG_RE_T RANSMIT	COUNTER	No	The sum of the total number of (interval) Register messages Re-Transmitted.	True	SUM
SUM_BYE_RETR ANSMIT	COUNTER	No	The sum of the total number of (interval) Bye messages Re-Transmitted.	True	SUM
SUM_CANCEL_R E_TRANSMIT	COUNTER	No	The sum of the total number of (interval) Cancel messages Re-Transmitted.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_OTHER_RE_TRANSMIT	COUNTER	No	The sum of the total number of (interval) Other messages Re-Transmitted.	True	SUM
SUM_RCV_MESSAGE	COUNTER	No	The sum of the total number of (interval) received Message method.	True	SUM
SUM_SND_MESSAGE	COUNTER	No	The sum of the total number of (interval) sent Message method.	True	SUM
SUM_RCV_PUBLISH	COUNTER	No	The sum of the total number of (interval) received Publish method.	True	SUM
SUM_SND_PUBLISH	COUNTER	No	The sum of the total number of (interval) sent Publish method.	True	SUM
SUM_EMERGENCY_ACCEPT	COUNTER	No	The sum of the total number of (interval) emergency calls accepted.	True	SUM
SUM_EMERGENCY_REJECT_BWCALL	COUNTER	No	The sum of the total number of (interval) emergency calls rejected because of bandwidth limit or call limit.	True	SUM
SUM_EMERGENCY_REJECT_POLICER	COUNTER	No	The sum of the total number of (interval) emergency calls rejected because of Priority Policer.	True	SUM
SUM_HPC_ACCEPT	COUNTER	No	The sum of the total number of (interval) HPC calls accepted.	True	SUM
SUM_NUM_OF_CALLS_SENDING_AARS	COUNTER	No	The sum of the number of calls sending AAR requests.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_OF_RECEIVED_AAA_FAILURES	COUNTER	No	The sum of the number of received AAA failures.	True	SUM
SUM_NUM_OF_TOTAL_AAR_SENT	COUNTER	No	The sum of the total number of AAR messages sent.	True	SUM
SUM_NUM_OF_TIMEOUT_OR_ERROR_AAR	COUNTER	No	The sum of the number of AAR messages not answered.	True	SUM
SUM_EMERGENCY_REG_ACCEPT	COUNTER	No	The sum of the number of (interval) emergency registrations accepted.	True	SUM
SUM_EMERGENCY_REG_REJECT_LIMIT	COUNTER	No	The sum of the number of (interval) emergency registrations rejected because of the registration limit.	True	SUM
SUM_EMERGENCY_REG_REJECT_POLICER	COUNTER	No	The sum of the number of (interval) emergency registrations rejected because of the Priority Policer.	True	SUM
SUM_PARSE_ERROR	COUNTER	No	The sum of the total number of (interval) Parse Errors.	True	SUM
SUM_NUM_OF_TOTAL_UDR_SENT	COUNTER	No	The sum of the total number of UDR messages sent.	True	SUM
SUM_NUM_OF_TIMEOUT_UDR_ERROR	COUNTER	No	The sum of the number of UDR messages not answered.	True	SUM
SUM_NUM_OF_RECEIVED_UDA_SUCCESS	COUNTER	No	The sum of the number of received UDA success.	True	SUM
SUM_NUM_OF_RECEIVED_UDA_FAILURES	COUNTER	No	The sum of the number of received UDA failures.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_TOTAL_NUM_S8HR_OUT_REG	COUNTER	No	The sum of the total number (includes success and failed) of registration received from S8HR Outbound Roaming Users.	True	SUM
SUM_NUM_S8HR_OUT_REG_SUC	COUNTER	No	The sum of the number of successful registration from S8HR Outbound Roaming Users.	True	SUM
SUM_NUM_S8HR_OUT_REG_FAIL	COUNTER	No	The sum of the number of S8HR Outbound Roaming Users registrations failed.	True	SUM
SUM_TOTAL_NUM_S8HR_OT_NML_CALL	COUNTER	No	The sum of the total number of normal calls initiated from S8HR Outbound Roaming Users.	True	SUM
SUM_NUM_OF_S8HR_OT_NML_CALL_SUC	COUNTER	No	The sum of the number of successful normal calls from S8HR Outbound Roaming Users.	Tru	SUM
SUM_NUM_OF_S8HR_OT_NML_CALL_FAIL	COUNTER	No	The sum of the total number of failed normal calls from S8HR Outbound Roaming Users.	True	SUM
SUM_NUM_OF_S8HR_OT_EMG_CALL_REJ	COUNTER	No	The sum of the number of S8HR Outbound Roaming User's emergency calls rejected.	True	SUM
SUM_NUM_OF_S8HR_IN_EMG_REG_SUC	COUNTER	No	The sum of the number of Successful registration from S8HR Inbound Roaming Users.	True	SUM
SUM_NUM_OF_S8HR_IN_EMG_REG_FAIL	COUNTER	No	The sum of the number of S8HR Inbound User's registration rejected.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_NUM_OF_S8HR_IN_EMG_CALL_SUC	COUNTER	No	The sum of the number of successful emergency calls from S8HR Inbound User.	True	SUM
SUM_NUM_OF_S8HR_IN_EMG_CALL_FAIL	COUNTER	No	The sum of the number of S8HR Inbound Users emergency calls failed.	True	SUM
SUM_NUM_OF_IN_HPC_CALL_ACC	COUNTER	No	The sum of the total number of (interval) Ingress HPC calls accepted.	True	SUM
SUM_NUM_OF_OUT_HPC_CALL_ACC	COUNTER	No	The sum of the total number of (interval) Egress HPC calls accepted.	True	SUM
SUM_NUM_OF_HPC_4XX_MSG_SENT	COUNTER	No	The sum of the total number of (interval) sent HPC 4xx messages.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

SipIpPeerOptionsIntervalStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
ACNAME	STRING	Yes	The name of the address context.	False	N/A	N/A
ZNAME	STRING	Yes	The name of this Zone.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_NAME	STRING	Yes	The name of this SIP IP Peer.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_DIRECTION	STRING	Yes	Indicates the direction of the (interval) SIP Options/Response messages.	False	N/A	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
SIP_IP_PEER_OPTIONS_MESSAGE	STRING	Yes	Indicates the cause code of the (interval) SIP Options/Response messages.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_MESSAGE_COUNT	COUNTER	No	Indicates the total number of (interval) SIP Options/Response messages for the specified cause code.	True	Sum	N/A
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A	N/A

SipIpPeerOptionsIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
ACNAME	STRING	Yes	The name of the address context.	False	N/A	N/A
ZNAME	STRING	Yes	The name of this Zone.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_NAME	STRING	Yes	The name of this SIP IP Peer.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_DIRECTION	STRING	Yes	Indicates the direction of the (interval) SIP Options/Response messages.	False	N/A	N/A
SIP_IP_PEER_OPTIONS_MESSAGE	STRING	Yes	Indicates the cause code of the (interval) SIP Options/Response messages.	False	N/A	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
SIP_IP_PEER_OPTIONS_MSG_COUNT	COUNTER	No	Indicates the total number of (interval) SIP Options/Response messages for the specified cause code.	True	Sum	N/A
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A	N/A

SipRegCountStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
NAME	INTEGER	Yes	Name of the system.	
SIP_REG_COUNT_ATTEMPTS	COUNTER	No	Indicates the number of SIP registration attempts.	
SIP_REG_COUNT_CUM_COMPLETIONS	COUNTER	No	Indicates the accumulative number of completed SIP registration attempts.	
SIP_REG_COUNT_PENDING	COUNTER	No	Indicates the current number of pending SIP registrations.	
SIP_REG_COUNT_STABLE	COUNTER	No	Indicates the current number of stable SIP registrations.	
SIP_REG_COUNT_TOTAL	COUNTER	No	Indicates the total number of current SIP registrations.	
SIP_EMERGENCY_REG_ACCEPT_TOTAL	COUNTER	No	Indicates the total number of accepted emergency SIP registrations.	

Column Name	Column Type	Index	Description	CLI Command Reference
SIP_EMERGENCY_REG_ACTIVE_TOTAL	COUNTER	No	Indicates the total number of active emergency SIP registrations.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

SipRegCountStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
NAME	INTEGER	Yes	Name of the system.	False	N/A
SUM_SIP_REG_COUNT_ATTEMPTS	COUNTER	No	The sum of the number of SIP registration attempts.	True	SUM
SUM_SIP_REG_COUNT_CUM_COMPLETIONS	COUNTER	No	The sum of the accumulative number of completed SIP registration attempts.	True	SUM
SUM_SIP_REG_COUNT_TOTAL	COUNTER	No	The sum of the total number of current SIP registrations.	True	SUM
SUM_SIP_EMERGENCY_REG_ACCEPT_TOTAL	COUNTER	No	The sum of the total number of accepted emergency SIP registrations.	True	SUM
AVG_SIP_EMERGENCY_REG_ACTIVE_TOTAL	GUAGE	No	Indicates the total number of emergency SIP registrations currently active.	True	MEAN
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

SipSigConnStatisticsStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	N/A
ZNAME	STRING	Yes	The name of the address context zone.	
IND	GAUGE	Yes	The index of this SIP Signaling Port.	
TCP_CONNECTION	COUNTER	No	Number of current TCP connections	
TOTAL_TCP_CONNECTION	COUNTER	No	Number of total TCP connections made.	
ACTIVE_TLS_TCP_CONNECTION	COUNTER	No	Number of current TLS-TCP connections made.	
TOTAL_TLS_TCP_CONNECTION	COUNTER	No	Number of total TLS-TCP connections.	
CE_NAME	STRING	No	The name of the compute element for this entry	

SipSigPortStatisticsStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context
ZNAME	STRING	Yes	The name of the address context zone.	
IND	GAUGE	Yes	The index of this SIP Signaling Port.	
CALL_RATE	INTEGER	No	Number of SIP calls per second during the last minute.	

Column Name	Column Type	Index	Description	CLI Command Reference
ORIG_CALLS	INTEGER	No	Total number of outgoing calls sent out from this signaling port.	
TERM_CALLS	INTEGER	No	Total number of incoming calls received on this signaling port.	
TX_PDUS	COUNTER64	No	The total number of signaling PDUS sent out on this port.	
RX_PDUS	COUNTER64	No	The total number of signaling PDUS received on this port.	
TX_BYTES	COUNTER64	No	The total number of signaling BYTES sent out from this port.	
RX_BYTES	COUNTER64	No	The total number of signaling BYTES received by this port.	
IN_REGS	INTEGER	No	Total number of inbound registration(s) received on this signaling port.	
OUT_REGS	INTEGER	No	Total number of outbound registration(s) sent on this signaling port.	
TX500S	INTEGER	No	The total number of 500 responses generated by the SLB when it is unable to forward a request.	
TX503S	INTEGER	No	The total number of 503 responses generated by the SLB when there are no backend SBCs able to handle the request due to the congestion or the cac restrictions.	

Column Name	Column Type	Index	Description	CLI Command Reference
CE_NAME	STRING	No	The name of the compute element for this entry.	

SipSigPortStatisticsStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
ZNAME	STRING	Yes	The name of the address context zone.	False	N/A
IND	GAUGE	Yes	The index of this SIP Signaling Port.	False	N/A
AVG_CALL_RATE	INTEGER	No	The average of the count of SIP calls per second during the last minute.	True	AVG
SUM_CALL_RATE	INTEGER	No	The sum of the count of SIP calls per second during the last minute.	True	SUM
AVG_ORIG_CALLS	INTEGER	No	The average of the count of outgoing calls sent out from this signaling port.	True	AVG
SUM_ORIG_CALLS	INTEGER	No	The sum of the count of outgoing calls sent out from this signaling port.	True	SUM
AVG_TERM_CALLS	INTEGER	No	The average of the count of incoming calls received on this signaling port.	True	AVG
SUM_TERM_CALLS	INTEGER	No	The sum of the count of incoming calls received on this signaling port.	True	SUM
AVG_TX_PDUS	INTEGER	No	The average of the count of signaling PDUS sent out on this port.	True	AVG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_TX_PDUS	INTEGER	No	The average of the count of signaling PDUS sent out on this port.	True	SUM
AVG_RX_PDUS	INTEGER	No	The average of the count of signaling PDUS received on this port.	True	AVG
SUM_RX_PDUS	INTEGER	No	The sum of the count of signaling PDUS received on this port.	True	SUM
AVG_TX_BYTES	INTEGER	No	The average of the count of signaling BYTES sent out from this port.	True	AVG
SUM_TX_BYTES	INTEGER	No	The sum of the count of signaling BYTES sent out from this port.	True	SUM
AVG_RX_BYTES	INTEGER	No	The average of the count of signaling BYTES received by this port.	True	AVG
SUM_RX_BYTES	INTEGER	No	The sum of the count of signaling BYTES received by this port.	True	SUM
AVG_IN_REGS	INTEGER	No	The average of the count of inbound registration(s) received on this signaling port.	True	AVG
SUM_IN_REGS	INTEGER	No	The sum of the count of inbound registration(s) received on this signaling port.	True	SUM
AVG_OUT_REGS	INTEGER	No	The average of the count of outbound registration(s) sent on this signaling port.	True	AVG
SUM_OUT_REGS	INTEGER	No	The sum of the count of outbound registration(s) sent on this signaling port.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
MEAN_TX500S	INTEGER	No	The total number of 500 responses generated by the SLB when it is unable to forward a request.	True	MEAN
MEAN_TX503S	INTEGER	No	The total number of 503 responses generated by the SLB when there are no backend SBCs able to handle the request due to the congestion or the cac restrictions.	True	MEAN
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

SipSigPortTlsStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	NA
ZNAME	STRING	Yes	The name of the address context zone.	
IND	GAUGE	Yes	The index of this SIP Signaling Port.	
CURRENT_CLIENT_SESSIONS	INTEGER	No	Number of client sessions currently active.	
CURRENT_SERVER_SESSIONS	INTEGER	No	Number of server sessions currently active.	
CURRENT_SUSPENDED_SESSIONS	INTEGER	No	Number of server sessions currently suspended.	
TOTAL_CLIENT_SESSIONS	INTEGER	No	Cumulative total number of client sessions.	
TOTAL_SERVER_SESSIONS	INTEGER	No	Cumulative total number of server sessions.	

Column Name	Column Type	Index	Description	CLI Command Reference
CURRENT_CLIENT_HANDSHAKES	INTEGER	No	Number of incomplete client handshakes.	
CURRENT_SERVER_HANDSHAKES	INTEGER	No	Number of incomplete server handshakes.	
SESSION_RESUMPTIONS	INTEGER	No	Number of resumed server sessions.	
NO_CIPHER_SUITE	INTEGER	No	Number of handshake failures due to inability to converge on a cipher suite.	
HANDSHAKE_TIMEOUTS	INTEGER	No	Number of handshakes that timed out before completing.	
HIGHER_AUTH_TIMEOUT	INTEGER	No	Number of handshakes in which the SBC was the server and the client did not authenticate itself through TLS and failed to authenticate itself through any higher level protocol (for example, SIP) before timing out.	
CLIENT_AUTH_FAILURES	INTEGER	No	Number of times peer failed TLS authentication with SBC as the client.	
SERVER_AUTH_FAILURES	INTEGER	No	Number of times peer failed TLS authentication with SBC as the server.	
FATAL_ALERTS_RECEIVED	INTEGER	No	Number of FATAL Alerts received.	
WARNING_ALERTS_RECEIVED	INTEGER	No	Number of WARNING Alerts received.	
HANDSHAKE_FAILURES	INTEGER	No	Cumulative total of all handshake failures.	

Column Name	Column Type	Index	Description	CLI Command Reference
RECEIVE_FAILURES	INTEGER	No	Number of receive failures (failure to decrypt).	
SEND_FAILURES	INTEGER	No	Number of send failures (failure to encrypt).	
NO_AUTH_DROPS	INTEGER	No	Number of SIP messages dropped due to lack of peer authentication at the SIP level.	
NO_AUTH488	INTEGER	No	Number of SIP messages rejected with 488 due to lack of peer authentication at the SIP level.	
MID_CONNECTION_HELLO	INTEGER	No	Number times a peer sent a TLS Hello on a connection that was already up (that is, the peer tried to renegotiate.).	
NO_CLIENT_CERT	INTEGER	No	Number times we were the client and we failed to derive a certificate to send the server.	
VALIDATION_FAILURES	INTEGER	No	Number of failed certificate validations.	
CURRENT_CLIENT_CONNECTIONS	INTEGER	No	Current number of client tls connections.	
TOTAL_CLIENT_CONNECTIONS	INTEGER	No	Cumulative total number of client tls connections.	
CURRENT_SERVER_CONNECTIONS	INTEGER	No	Current number of server tls connections.	
TOTAL_SERVER_CONNECTIONS	INTEGER	No	Cumulative total number of server tls connections.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

SipSubCountStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context
NAME	INTEGER	Yes	Name of the system.	False	
SIP_SUB_COUNT_ATTEMPTS	COUNTER	No	Indicates the number of SIP relayed subscription attempts.	True	
SIP_SUB_COUNT_CUM_COMPLETIONS	COUNTER	No	Indicates the accumulative number of completed SIP subscription attempts.	True	
SIP_SUB_COUNT_STABLE	COUNTER	No	Indicates the current number of stable SIP subscription.	True	
SIP_SUB_COUNT_TOTAL	COUNTER	No	Indicates the total number of current SIP subscription on this card (SIP_SUB_COUNT_ATTEMPTS + SIP_SUB_COUNT_CUM_COMPLETIONS)	True	
SIP_SUB_COUNT_FAILURE	COUNTER	No	Indicates the number of SIP relayed subscription failures.	False	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

SipSubCountStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type (SUM/AVG)
ACNAME	STRING	Yes	The name of the address context.	False	N/A

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type (SUM/AVG)
NAME	INTEGER	Yes	Name of the system.	False	N/A
SUM_SIP_SUB_COUNT_ATTEMPTS	COUNTER	No	The sum of the number of SIP relayed subscription attempts.	True	SUM
SUM_SIP_SUB_COUNT_CUM_COMPLETIONS	COUNTER	No	The sum of the accumulative number of completed SIP subscription attempts.	True	SUM
AVG_SIP_SUB_COUNT_STABLE	GAUGE	No	The current number of stable SIP subscription on this card.	True	MEAN
SIP_SUB_COUNT_FAILURE	COUNTER	No	Indicates the number of SIP relayed subscription failures.	False	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

SipTrunkGroupOptionsIntervalStats

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
ACNAME	STRING	Yes	The name of the address context.	False	N/A	No
ZNAME	STRING	Yes	The name of this zone.	False	N/A	No
SIP_TG_OPTIONS_NAME	STRING	Yes	The name of this SIP trunk group.	False	N/A	No
SIP_TG_OPTIONS_DIRECTION	STRING	Yes	The direction of the (interval) SIP Options/Response messages.	False	N/A	No

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
SIP_TG_OPTIONS_MESSAGE	STRING	Yes	The cause code of the (interval) SIP Options/Response messages.	False	N/A	No
SIP_TG_OPTIONS_MSG_COUNT	COUNTER	No	The total number of (interval) SIP Options/Response messages for the specified cause code.	True	SUM	No
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A	No

SipTrunkGroupOptionsIntervalStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
ACNAME	STRING	Yes	The name of the address context.	False	N/A	No
ZNAME	STRING	Yes	The name of this zone.	False	N/A	No
SIP_TG_OPTIONS_NAME	STRING	Yes	The name of this SIP trunk group.	False	N/A	No
SIP_TG_OPTIONS_DIRECTION	STRING	Yes	The direction of the (interval) SIP Options/Response messages.	False	N/A	No
SIP_TG_OPTIONS_MESSAGE	STRING	Yes	The cause code of the (interval) SIP Options/Response messages.	False	N/A	No
SIP_TG_OPTIONS_MSG_COUNT	COUNTER	No	The total number of (interval) SIP Options/Response messages for the specified cause code.	True	SUM	No

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type	Present in Post Paid Reports
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A	No

SystemLicenseInfoStats

Note

SystemLicenseInfoStats is available only if SBC 3.1 Device Manager is installed.

Column Name	Column Type	Index	Description	CLI Command Reference
FEATURE_NAME	STRING	Yes	This object indicates the feature name.	Show Table System
LICENSE_ID	STRING	Yes	This object indicates the license Id.	
EXPIRATION_DATE	STRING	No	This object indicates the license expiry date for a feature.	
USAGE_LIMIT	INTEGER	No	This object indicates the usage limit of a feature.	
SOURCE	STRING	No	This object indicates where the licenses is located, nodeLocked or domain.	
IN_USE	GAUGE	No	This object indicates the number of licenses used by the application.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

TrafficControlStats

Column Name	Column Type	Index	Description	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	Show Table Address Context

Column Name	Column Type	Index	Description	CLI Command Reference
ZNAME	STRING	Yes	The name of the address context zone.	
NAME	STRING	Yes	The name of this trunk group.	
SILC	GAUGE	No	The number of calls cancelled due to SILC for this trunk group for the specified interval.	
STR_CANT	GAUGE	No	The number of calls cancelled due to STR for this trunk group for the specified interval.	
STR_SKIP	GAUGE	No	The number of calls skipped due to STR for this trunk group for the specified interval.	
SKIP	GAUGE	No	The number calls skipped due to the SKIP traffic control for this trunk group for the specified interval.	
CANT	GAUGE	No	The number of calls cancelled due to CANT for this trunk group for the specified interval.	
CANF	GAUGE	No	The number of calls cancelled due to CANF for this trunk group for the specified interval.	
ACC_CANT	GAUGE	No	The number of calls cancelled due to ACC for this trunk group for the specified interval.	
ACC_SKIP	GAUGE	No	The number of calls skipped due to ACC for this trunk group for the specified interval.	

Column Name	Column Type	Index	Description	CLI Command Reference
ROUTE_ATTEMPTS_IRR	GAUGE	No	The number of reroute attempts due to IRR for this trunk group for the specified interval.	
ROUTE_ATTEMPTS_SIRR	GAUGE	No	The number of reroute attempts due to SIRR for this trunk group for the specified interval.	
ROUTE_ATTEMPTS_ORR	GAUGE	No	The number of reroute attempts due to ORR for this trunk group for the specified interval.	
ROUTE_ATTEMPTS_SORR	GAUGE	No	The number of reroute attempts due to SORR for this trunk group for the specified interval.	
SUCCESSFUL_IRR	GAUGE	No	The number of successful reroutes due to IRR for this trunk group for the specified interval.	
SUCCESSFUL_SIRR	GAUGE	No	The number of successful reroutes due to SIRR for this trunk group for the specified interval.	
SUCCESSFUL_ORR	GAUGE	No	The number of successful reroutes due to ORR for this trunk group for the specified interval.	
SUCCESSFUL_SORR	GAUGE	No	The number of successful reroutes due to SORR for this trunk group for the specified interval.	
CE_NAME	STRING	No	The name of the compute element for this entry.	

ZoneIntervalStatisticsStats

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
ACNAME	STRING	Yes	The name of the address context.	False	Show Table Address Context
NAME	STRING	Yes	The name of this zone.	False	
INGRESS_FAIL_CALL_LIMIT	COUNTER	No	Number of incoming calls failed due to Call Limit check on Zone.	False	
EGRESS_FAIL_CALL_LIMIT	COUNTER	No	Number of outgoing calls failed due to Call Limit check on Zone.	False	
INGRESS_FAIL_CALL_POLICING	COUNTER	No	Number of incoming calls failed due to Call Policer check on Zone.	False	
EGRESS_FAIL_CALL_POLICING	COUNTER	No	Number of outgoing calls failed due to Call Policer check on Zone.	False	
INGRESS_FAIL_BWLIMIT	COUNTER	No	Number of incoming calls failed due to Bandwidth Limit check on Zone.	False	
EGRESS_FAIL_BWLIMIT	COUNTER	No	Number of outgoing calls failed due to Bandwidth Limit check on Zone.	False	
INGRESS_SIP_REG_FAIL_LIMIT	COUNTER	No	Number of incoming SIP Registrations failed due to Registrations Limit check on Zone.	False	

Column Name	Column Type	Index	Description	canAggregate	CLI Command Reference
EGRESS_SIP_REG_FAIL_LIMIT	COUNTER	No	Number of outgoing SIP Registrations failed due to Registrations Limit check on Zone.	False	
INGRESS_SIP_REG_POLICING	COUNTER	No	Number of incoming SIP Registrations failed due to ingress Policer check on Zone.	False	
EGRESS_SIP_REG_POLICING	COUNTER	No	Number of outgoing SIP Registrations failed due to egress Policer check on Zone.	False	
VIDEO_THRESHOLD_LIMIT	COUNTER	No	The number of exceeded video threshold limits for this zone.	True	
CE_NAME	STRING	No	The name of the compute element for this entry.	False	

ZoneIntervalStatisticsStats_AG

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
ACNAME	STRING	Yes	The name of the address context.	False	N/A
NAME	STRING	Yes	The name of this zone.	False	N/A
SUM_INGRESS_FAIL_CALL_LIMIT	COUNTER	No	The sum of the number of incoming calls failed due to Call Limit check on Zone.	True	SUM
SUM_EGRESS_FAIL_CALL_LIMIT	COUNTER	No	The sum of the number of outgoing calls failed due to Call Limit check on Zone.	True	SUM

Column Name	Column Type	Index	Description	canAggregate	Aggregate Type
SUM_INGRESS_FAIL_CALL_POLICYING	COUNTER	No	The sum of the number of incoming calls failed due to Call Policer check on Zone.	True	SUM
SUM_EGRESS_FAIL_CALL_POLICYING	COUNTER	No	The sum of the number of outgoing calls failed due to Call Policer check on Zone.	True	SUM
SUM_INGRESS_FAIL_BWLIMIT	COUNTER	No	The sum of the number of incoming calls failed due to Bandwidth Limit check on Zone.	True	SUM
SUM_EGRESS_FAIL_BWLIMIT	COUNTER	No	The sum of the number of outgoing calls failed due to Bandwidth Limit check on Zone.	True	SUM
SUM_INGRESS_SIP_REG_FAIL_LIMIT	COUNTER	No	The sum of the number of incoming SIP Registrations failed due to Registrations Limit check on Zone.	True	SUM
SUM_EGRESS_SIP_REG_FAIL_LIMIT	COUNTER	No	The sum of the number of outgoing SIP Registrations failed due to Registrations Limit check on Zone.	True	SUM
SUM_INGRESS_SIP_REG_POLICYING	COUNTER	No	The sum of the number of incoming SIP Registrations failed due to ingress Policer check on Zone.	True	SUM
SUM_EGRESS_SIP_REG_POLICYING	COUNTER	No	The sum of the number of outgoing SIP Registrations failed due to egress Policer check on Zone.	True	SUM
CE_NAME	STRING	No	The name of the compute element for this entry.	False	N/A

SLB Statistics

In this section:

- [SLBAclOffListIntStats](#)
- [SLBAggregateOffIntStats](#)
- [SLBArpOffListIntStats](#)
- [SLBBadEtherIpHdrOffIntStats](#)
- [SLBDiscardRuleOffIntStats](#)
- [SLBEthernetPortMgmtStats](#)
- [SLBEthernetPortPacketPortStatus](#)
- [SLBEthernetPortPacketStats](#)
- [SLBicmpGeneralGroupStats](#)
- [SLBIntervalStatistics](#)
- [SLBIpAclOverallStats](#)
- [SLBIpAclRuleStats](#)
- [SLBIpGeneralGroupStats](#)
- [SLBIpPolicingSystemIntStats](#)
- [SLBIpSecDecryptOffIntStats](#)
- [SLBLicenseUsageStats](#)
- [SLBLinkDetectionGroupStats](#)
- [SLBLinkMonitorStats](#)
- [SLBSipSigConnStatisticsStats](#)
- [SLBSipSigPortStatisticsStats](#)
- [SLBSysCpuUtilIntStatsSts](#)
- [SLBSysMemoryUtilIntStatsSts](#)
- [SLBSystemCongestionIntervalStats](#)
- [SLBSystemLicenseInfoStats](#)
- [SLBTcpGeneralGroupStats](#)
- [SLBUdpGeneralGroupStats](#)
- [SLBUflowOffListIntStats](#)

SLBAclOffListIntStats

Column Name	Column Type	Index	Description	canAggregate
ROLE	INTEGER	true	Role of the system.	false
SERIAL_INDEX	INTEGER	true	The index of the system	false
ADDRESS_CONTEXT	STRING	false	The name of the address context of the table entry	false
INTERFACE_GROUP_NAME	STRING	false	The name of the interface group of the table entry	false
INTERFACE_NAME	STRING	false	The name of the interface of the table entry	false

Column Name	Column Type	Index	Description	canAggregate
SOURCE_IP_ADDRESS	STRING	false	The source IP address of the table entry	false
DEST_IP_ADDRESS	STRING	false	The dest IP address of the table entry	false
SOURCE_IP_PORT	INTEGER	false	The source IP port of the table entry	false
DEST_IP_PORT	INTEGER	false	The dest IP port of the table entry	false
IP_PROTOCOL	INTEGER	false	The IP Protocol of the table entry	false
DISCARD_COUNT	COUNTER	false	The number of packets discarded by the policer	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBAggregateOffIntStats

Column Name	Column Type	Index	Description	canAggregate
ROLE	INTEGER	true	Role of the system.	false
SERIAL_INDEX	INTEGER	true	The index of the system	false
ADDRESS_CONTEXT	STRING	false	The name of the address context of the table entry	false
INTERFACE_GROUP_NAME	STRING	false	The name of the interface group of the table entry	false
INTERFACE_NAME	STRING	false	The name of the interface of the table entry	false
SOURCE_IP_ADDRESS	STRING	false	The source IP address of the table entry	false
DEST_IP_ADDRESS	STRING	false	The dest IP address of the table entry	false

Column Name	Column Type	Index	Description	canAggregate
SOURCE_IP_PORT	INTEGER	false	The source IP port of the table entry	false
DEST_IP_PORT	INTEGER	false	The dest IP port of the table entry	false
IP_PROTOCOL	INTEGER	false	The IP Protocol of the table entry	false
DISCARD_COUNT	COUNTER	false	The number of packets discarded by the policer	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBArpOffListIntStats

Column Name	Column Type	Index	Description	canAggregate
ROLE	INTEGER	true	Role of the system.	false
SERIAL_INDEX	INTEGER	true	The index of the system	false
ADDRESS_CONTEXT	STRING	false	The name of the address context of the table entry	false
INTERFACE_GROUP_NAME	STRING	false	The name of the interface group of the table entry	false
INTERFACE_NAME	STRING	false	The name of the interface of the table entry	false
SOURCE_IP_ADDRESS	STRING	false	The source IP address of the table entry	false
DEST_IP_ADDRESS	STRING	false	The dest IP address of the table entry	false
IP_PROTOCOL	INTEGER	false	The IP Protocol of the table entry	false
DISCARD_COUNT	COUNTER	false	The number of packets discarded by the policer	false

Column Name	Column Type	Index	Description	canAggregate
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBBadEtherIpHdrOffIntStats

Column Name	Column Type	Index	Description	canAggregate
ROLE	INTEGER	true	Role of the system.	false
SERIAL_INDEX	INTEGER	true	The index of the system	false
ADDRESS_CONTEXT	STRING	false	The name of the address context of the table entry	false
INTERFACE_GROUP_NAME	STRING	false	The name of the interface group of the table entry	false
INTERFACE_NAME	STRING	false	The name of the interface of the table entry	false
SOURCE_IP_ADDRESS	STRING	false	The source IP address of the table entry	false
DEST_IP_ADDRESS	STRING	false	The dest IP address of the table entry	false
SOURCE_IP_PORT	INTEGER	false	The source IP port of the table entry	false
DEST_IP_PORT	INTEGER	false	The dest IP port of the table entry	false
IP_PROTOCOL	INTEGER	false	The IP Protocol of the table entry	false
ETHER_TYPE	COUNTER	false	The first ethertype found in the Ethernet packet	false
DISCARD_COUNT	COUNTER	false	The number of packets discarded by the policer	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBDiscardRuleOffIntStats

Column Name	Column Type	Index	Description	canAggregate
ROLE	INTEGER	true	Role of the system.	false
SERIAL_INDEX	INTEGER	true	The index of the system	false
ADDRESS_CONTEXT	STRING	false	The name of the address context of the table entry	false
INTERFACE_GROUP_NAME	STRING	false	The name of the interface group of the table entry	false
INTERFACE_NAME	STRING	false	The name of the interface of the table entry	false
SOURCE_IP_ADDRESS	STRING	false	The source IP address of the table entry	false
DEST_IP_ADDRESS	STRING	false	The dest IP address of the table entry	false
SOURCE_IP_PORT	INTEGER	false	The source IP port of the table entry	false
DEST_IP_PORT	INTEGER	false	The dest IP port of the table entry	false
IP_PROTOCOL	INTEGER	false	The IP Protocol of the table entry	false
DISCARD_COUNT	COUNTER	false	The number of packets discarded by the policer	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBEthernetPortMgmtStats

Column Name	Column Type	Index	Description	canAggregate
PORT_NAME	STRING	true	The name of this port.	false

Column Name	Column Type	Index	Description	canAggregate
RX_PACKETS	COUNTER64	false	The number of received packets.	false
TX_PACKETS	COUNTER64	false	The number of transmitted packets.	false
RX_ERRORS	COUNTER	false	The number of bad packets received	false
TX_ERRORS	COUNTER	false	The number of packet transmit failures.	false
RX_DROPPED	COUNTER	false	The number of packets dropped due to no receive buffers.	false
TX_DROPPED	COUNTER	false	The number of packets dropped due to no transmit buffers.	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBEthernetPortPacketPortStatus

Column Name	Column Type	Index	Description	canAggregate
AVG_RX_ACTUAL_BW	GAUGE	False	Tracks the Average Incoming Bandwidth used during KPI bin interval in bytes/sec.	True
AVG_TX_ACTUAL_BW	GAUGE	False	Tracks the Average Outgoing Bandwidth used during KPI bin interval in bytes/sec.	True
PEAK_RX_ACTUAL_BW	GAUGE	False	Tracks the Peak Incoming Bandwidth used during KPI bin interval in bytes/sec.	True
PEAK_TX_ACTUAL_BW	GAUGE	False	Tracks the Peak Outgoing Bandwidth used during KPI bin interval in bytes/sec.	True
AVG_RX_ACTUAL_BWUTIL	GAUGE	False	Tracks the average incoming BW utilization based on total available port BW instead of negotiated BW.	True

Column Name	Column Type	Index	Description	canAggregate
PEAK_RX_ACTUAL_BWUTIL	Gauge	False	Tracks the maximum incoming BW utilization during the KPI bin interval expressed as a percentage of the available BW.	True
AVG_TX_ACTUAL_BWUTIL	Gauge	False	Tracks the average outgoing BW utilization during the KPI bin interval based on total available BW instead of negotiated BW.	True
PEAK_TX_ACTUAL_BWUTIL	Gauge	False	Tracks the maximum outgoing BW utilization during the KPI bin interval expressed as a percentage of the available BW.	True
BWALARM_THRESHOLD_EXCEEDED	Gauge	False	Tracks the total number of times the BW alarm threshold was passed in the upward direction during the bin interval	True
BWALARM_CLEARED	Gauge	False	Tracks the total number of times the BW clear alarm threshold was passed in the downward direction during the bin interval.	True
AVG_USAGE_BW	Gauge	False	Tracks the Average Bandwidth Usage during KPI bin interval	True
PEAK_USAGE_BW	Gauge	False	Tracks the Peak Bandwidth Usage during KPI bin interval.	True
CE_NAME	String	True	The host name of the server.	False
PORT_NAME	String	True	The name of this port.	False
NEGOTIATED_SPEED	Integer	False	The interface speed. Packet port speed is not negotiable.	True
LINK_STATE	Integer	False	The state of the interface.	True
MAX_BANDWIDTH	Gauge	False	Maximum bandwidth this port can support, bytes/sec.	True
ALLOCATED_BANDWIDTH	Gauge	False	Bandwidth the active media streams on this port reserve, bytes/sec.	True
RX_BANDWIDTH	Gauge	False	Actual Rx bandwidth in use on this port, bytes/sec.	True

Column Name	Column Type	Index	Description	canAggregate
TX_BANDWIDTH	Gauge	False	Actual Tx bandwidth in use on this port, bytes/sec.	True
BANDWIDTH_USAGE	Gauge	False	Percentage of maximum bandwidth allocated on this port.	True
BANDWIDTH_DEVIATION	Gauge	False	Percentage of deviation of actual bandwidth from the allocated bandwidth.	True
MAC_ADDRESS	STRING	False	The MAC address of the network interface.	False
IF_INDEX	Gauge	False	The unique ifIndex of this Packet NIF.	True

SLBEthernetPortPacketStats

Column Name	Column Type	Index	Description	canAggregate
PORT_NAME	STRING	true	The name of this port.	false
RX_PACKETS	COUNTER64	false	The number of received packets.	false
TX_PACKETS	COUNTER64	false	The number of transmitted packets.	false
RX_ERRORS	COUNTER	false	The number of bad packets received	false
TX_ERRORS	COUNTER	false	The number of packet transmit failures.	false
RX_DROPPED	COUNTER	false	The number of packets dropped due to no receive buffers.	false
TX_DROPPED	COUNTER	false	The number of packets dropped due to no transmit buffers.	false
RX_BYTES	COUNTER64	false	The number of received bytes.	false

Column Name	Column Type	Index	Description	canAggregate
TX_BYTES	COUNTER64	false	The number of transmitted bytes.	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBIcmpGeneralGroupStats

Column Name	Column Type	Index	Description	canAggregate
CE_NAME	STRING	true	The name of the compute element for this entry.	false
IN_MSGS	COUNTER	false	The total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.	false
IN_ECHOS	COUNTER	false	The number of ICMP Echo (request) messages received.	false
IN_ECHO_REPS	COUNTER	false	The number of ICMP Echo Reply messages received.	false
IN_DEST_UNREACHS	COUNTER	false	The number of ICMP Destination Unreachable messages received.	false
IN_ERRORS	COUNTER	false	The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).	false
OUT_MSGS	COUNTER	false	The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOutErrors.	false

Column Name	Column Type	Index	Description	canAggregate
OUT_ERRORS	COUNTER	false	The number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.	false
OUT_ECHOS	COUNTER	false	The number of ICMP Echo (request) messages sent.	false
OUT_ECHO_REPS	COUNTER	false	The number of ICMP Echo Reply messages sent.	false
OUT_DEST_UNREACHS	COUNTER	false	The number of ICMP Destination Unreachable messages sent.	false

SLBIntervalStatistics

Column Name	Column Type	Index	Description	canAggregate
ID	GAUGE	true	Instance id of the SIP client.	false
VNFID	STRING	false	The VNF ID of the SIP client.	false
MSGSENT	COUNTER	false	Number of messages sent to the SIP client.	false
INVITE_MSGSENT	COUNTER	false	Number of INVITEs sent to the SIP client.	false
OOD_MSGSENT	COUNTER	false	Number of out-of-dialog requests sent to the SIP client.	false
REGISTER_MSGSENT	COUNTER	false	Number of out-of-register requests sent to the SIP client.	false
CE_NAME	STRING	false	The name of the compute element for this entity.	false

SLBIPAcIOverallStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	true	The name of the address context.	false
NAME	IMPLIEDSTRING	true	The name of the address context.	false
MATCHED_NO_RULE	COUNTER	false	The number of times no rule matches.	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBIPAcIRuleStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	true	The name of the address context.	false
NAME	STRING	true	The name of this IP access control list rule.	false
MATCHES	COUNTER	false	The number of times this rule has been matched.	false
POLICER_DISCARDS	COUNTER	false	The number of times the policer for this rule discarded packets.	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBIPGeneralGroupStats

Column Name	Column Type	Index	Description	canAggregate
CE_NAME	STRING	true	The name of the compute element for this entry.	false
IN_RECEIVES	COUNTER	false	The total number of input datagrams received from interfaces, including those received in error.	false

Column Name	Column Type	Index	Description	canAggregate
IN_HDR_ERRORS	COUNTER	false	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.	false
IN_ADDR_ERRORS	COUNTER	false	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., 0.0.0.0) and addresses of unsupported Classes (e.g., Class E). For entities which are not IP routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.	false
IN_UNKNOWN_PROTOS	COUNTER	false	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.	false
IN_DISCARDS	COUNTER	false	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.	false
IN_DELIVERS	COUNTER	false	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).	false
OUT_REQUESTS	COUNTER	false	The total number of IP datagrams which local IP user- protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.	false

Column Name	Column Type	Index	Description	canAggregate
OUT_DISCARDS	COUNTER	false	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.	false
OUT_NO_ROUTE ES	COUNTER	false	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in ipForwDatagrams which meet this 'no-route' criterion. Note that this includes any datagrams which a host cannot route because all of its default routers are down.	false
REASM_TIMEOUT	INTEGER	false	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.	false
REASM_REQDS	COUNTER	false	The number of IP fragments received which needed to be reassembled at this entity.	false
REASM_OKS	COUNTER	false	The number of IP datagrams successfully re-assembled.	false
REASM_FAILS	COUNTER	false	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.	false
FRAG_OKS	COUNTER	false	The number of IP datagrams that successfully fragmented at this entity.	false
FRAG_FAILS	COUNTER	false	The number of discarded IP datagrams that were not successfully fragmented due to some issue (e.g., the Don't Fragment flag was set).	false

SLBIPolicingSystemIntStats

Column Name	Column Type	Index	Description	canAggregate
SYSTEM_NAME	STRING	true	Name of the system.	false
BAD_HDR_DISCARD_PACKET_COUNT	COUNTER64	false	The current number of discarded packets for the bad Ethernet/IP Header policer.	false
BAD_HDR_PEAK_DISCARD_RATE	GAUGE	false	The current peak discard rate for the bad Ethernet/IP Header policer.	false
BAD_HDR_MINOR_ALARM_COUNT	GAUGE	false	The current number of minor alarms for the bad Ethernet/IP Header policer.	false
BAD_HDR_MINOR_ALARM_DURATION	GAUGE	false	The current duration of the minor alarms in seconds for the bad Ethernet/IP Header policer.	false
BAD_HDR_MAJOR_ALARM_COUNT	GAUGE	false	The current number of major alarms for the bad Ethernet/IP Header policer.	false
BAD_HDR_MAJOR_ALARM_DURATION	GAUGE	false	The current duration of the major alarms in seconds for the bad Ethernet/IP Header policer.	false
ARP_DISCARD_PACKET_COUNT	COUNTER64	false	The current number of discarded packets for the ARP policer.	false
ARP_ACCEPT_PACKET_COUNT	COUNTER64	false	The current number of discarded packets for the ARP policer.	false
ARP_PEAK_DISCARD_RATE	GAUGE	false	The current peak discard rate for the ARP policer.	false
ARP_MINOR_ALARM_COUNT	GAUGE	false	The current number of minor alarms for the ARP policer.	false
ARP_MINOR_ALARM_DURATION	GAUGE	false	The current duration of the minor alarms in seconds for the ARP policer.	false

Column Name	Column Type	Index	Description	canAggregate
ARP_MAJOR_ALARM_COUNT	GAUGE	false	The current number of major alarms for the ARP policer.	false
ARP_MAJOR_ALARM_DURATION	GAUGE	false	The current duration of the major alarms in seconds for the ARP policer.	false
UFLOW_DISCARD_PACKET_COUNT	COUNTER64	false	The current number of discarded packets for the micro flow policer.	false
UFLOW_ACCEPT_PACKET_COUNT	COUNTER64	false	The current number of discarded packets for the micro flow policer.	false
UFLOW_PEAK_DISCARD_RATE	GAUGE	false	The current peak discard rate for the micro flow policer.	false
UFLOW_MINOR_ALARM_COUNT	GAUGE	false	The current number of minor alarms for the micro flow policer.	false
UFLOW_MINOR_ALARM_DURATION	GAUGE	false	The current duration of the minor alarms in seconds for the micro flow policer.	false
UFLOW_MAJOR_ALARM_COUNT	GAUGE	false	The current number of major alarms for the micro flow policer.	false
UFLOW_MAJOR_ALARM_DURATION	GAUGE	false	The current duration of the major alarms in seconds for the micro flow policer.	false
ACL_DISCARD_PACKET_COUNT	COUNTER64	false	The current number of discarded packets for the access control list policer.	false
ACL_ACCEPT_PACKET_COUNT	COUNTER64	false	The current number of discarded packets for the access control list policer.	false
ACL_PEAK_DISCARD_RATE	GAUGE	false	The current peak discard rate for the access control list policer.	false

Column Name	Column Type	Index	Description	canAggregate
ACL_MINOR_ALARM_COUNT	GAUGE	false	The current number of minor alarms for the access control list policer.	false
ACL_MINOR_ALARM_DURATION	GAUGE	false	The current duration of the minor alarms in seconds for the access control list policer.	false
ACL_MAJOR_ALARM_COUNT	GAUGE	false	The current number of major alarms for the access control list policer.	false
ACL_MAJOR_ALARM_DURATION	GAUGE	false	The current duration of the major alarms in seconds for the access control list policer.	false
AGGREGATE_DISCARD_PKT_COUNT	COUNTER64	false	The current number of discarded packets for the aggregate policer.	false
AGGREGATE_ACCEPT_PKT_COUNT	COUNTER64	false	The current number of discarded packets for the aggregate policer.	false
AGGREGATE_PEAK_DISCARD_RATE	GAUGE	false	The current peak discard rate for the aggregate policer.	false
AGGREGATE_MINOR_ALARM_COUNT	GAUGE	false	The current number of minor alarms for the aggregate policer.	false
AGGREGATE_MINOR_ALARM_DUR	GAUGE	false	The current duration of the minor alarms in seconds for the aggregate policer.	false
AGGREGATE_MAJOR_ALARM_COUNT	GAUGE	false	The current number of major alarms for the aggregate policer.	false
AGGREGATE_MAJOR_ALARM_DUR	GAUGE	false	The current duration of the major alarms in seconds for the aggregate policer.	false
MEDIA_DISCARD_PACKET_COUNT	COUNTER64	false	The current number of discarded packets for the media policer.	false

Column Name	Column Type	Index	Description	canAggregate
MEDIA_PEAK_DISCARD_RATE	GAUGE	false	The current peak discard rate for the media policer.	false
MEDIA_MINOR_ALARM_COUNT	GAUGE	false	The current number of minor alarms for the media policer.	false
MEDIA_MINOR_ALARM_DURATION	GAUGE	false	The current duration of the minor alarms in seconds for the media policer.	false
MEDIA_MAJOR_ALARM_COUNT	GAUGE	false	The current number of major alarms for the media policer.	false
MEDIA_MAJOR_ALARM_DURATION	GAUGE	false	The current duration of the major alarms in seconds for the media policer.	false
ROGUE_MEDIA_DISCARD_PKT_COUNT	COUNTER64	false	The current number of discarded packets for the rogue media policer.	false
ROGUE_MEDIA_PEAK_DISCARD_RATE	GAUGE	false	The current peak discard rate for the rogue media policer.	false
ROGUE_MEDIA_MINOR_ALARM_COUNT	GAUGE	false	The current number of minor alarms for the rogue media policer.	false
ROGUE_MEDIA_MINOR_ALARM_DURATION	GAUGE	false	The current duration of the minor alarms in seconds for the rogue media policer.	false
ROGUE_MEDIA_MAJOR_ALARM_COUNT	GAUGE	false	The current number of major alarms for the rogue media policer.	false
ROGUE_MEDIA_MAJOR_ALARM_DURATION	GAUGE	false	The current duration of the major alarms in seconds for the rogue media policer.	false
DISCARD_RULE_PACKET_COUNT	COUNTER64	false	The current number of discarded packets for the IPSEC Decrypt policer.	false
DISCARD_PEAK_DISCARD_RATE	GAUGE	false	The current peak discard rate for the discard rule.	false

Column Name	Column Type	Index	Description	canAggregate
DISCARD_MINOR_ALARM_COUNT	GAUGE	false	The current number of minor alarms for the discard rule.	false
DISCARD_MINOR_ALARM_DURATION	GAUGE	false	The current duration of the minor alarms in seconds for the discard rule.	false
DISCARD_MAJOR_ALARM_COUNT	GAUGE	false	The current number of major alarms for the discard rule.	false
DISCARD_MAJOR_ALARM_DURATION	GAUGE	false	The current duration of the major alarms in seconds for the discard rule.	false
DECRYPT_DISCARD_PACKET_COUNT	COUNTER64	false	The current number of packets discarded by SRTP decrypt discards.	false
PEAK_DECRYPT_DISCARD_RATE	GAUGE	false	The current peak discard rate for SRTP decrypt discards.	false
MINOR_DECRYPT_ALARM_COUNT	INTEGER	false	The current number of minor alarms for SRTP decrypt discards.	false
MINOR_DECRYPT_ALARM_DURATION	INTEGER	false	The current duration of the minor alarms in seconds for SRTP decrypt discards.	false
MAJOR_DECRYPT_ALARM_COUNT	INTEGER	false	The current number of major alarms for the SRTP decrypt discards.	false
MAJOR_DECRYPT_ALARM_DURATION	INTEGER	false	The current duration of the major alarms in seconds for SRTP decrypt discards.	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBIPSecDecryptOffIntStats

Column Name	Column Type	Index	Description	canAggregate
ROLE	INTEGER	true	Role of the system.	false
SERIAL_INDEX	INTEGER	true	The index of the system	false
ADDRESS_CONTEXT	STRING	false	The name of the address context of the table entry	false
INTERFACE_GROUP_NAME	STRING	false	The name of the interface group of the table entry	false
INTERFACE_NAME	STRING	false	The name of the interface of the table entry	false
SOURCE_IP_ADDRESS	STRING	false	The source IP address of the table entry	false
DEST_IP_ADDRESS	STRING	false	The dest IP address of the table entry	false
SOURCE_IP_PORT	INTEGER	false	The source IP port of the table entry	false
DEST_IP_PORT	INTEGER	false	The dest IP port of the table entry	false
IP_PROTOCOL	INTEGER	false	The IP Protocol of the table entry	false
DISCARD_COUNT	COUNTER	false	The number of packets discarded by the policer	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBLicenseUsageStats

Column Name	Column Type	Index	Description	canAggregate
FEATURE_NAME	INTEGER	true	A dummy key is added to the non-config scalar element container even though only one row is allowed in a container. Without the key, tailf treats the container as non-dynamic and calls the get_elem per leaf instead of calling the get_object per row.	false
LICENSE_MODE	STRING	false	Displays the licensing mode of SBC.	false
ENCRYPT_ENABLED	INTEGER	false	Set based on whether encrypt license is available at the SBC.	false
SRTP_ENABLED	INTEGER	false	Set based on whether srtp license is available at the SBC.	false
VIDEO_ENABLED	INTEGER	false	Set based on whether video license is available at the SBC.	false
AMRNB_ENABLED	INTEGER	false	Set based on whether amrnb license is available at the SBC.	false
AMRWB_ENABLED	INTEGER	false	Set based on whether amrwb license is available at the SBC.	false
EVRC_ENABLED	INTEGER	false	Set based on whether evrc license is available at the SBC.	false
NICE_ENABLED	INTEGER	false	Set based on whether nicerec license is available at the SBC	false
MRF_ENABLED	INTEGER	false	Set based on whether mrf license is available at the SBC.	false
SIPREC_ENABLED	INTEGER	false	Set based on whether siprec license is available at the SBC.	false
VDSPRTU_ENABLED	INTEGER	false	Set based on whether transcode license is available at the SBC.	false
PDCS_ENABLED	INTEGER	false	Set based on whether pdcs license is available at the SBC.	false

Column Name	Column Type	Index	Description	canAggregate
LI_ENABLED	INTEGER	false	Set based on whether LI license is available at the SBC.	false
RTU_ENABLED	INTEGER	false	Set based on whether SbcRtu license is available at the SBC.	false
DSPG722_ENABLED	INTEGER	false	Set based on whether DspG722 license is available at the SBC.	false
GMP4X1_ENABLED	INTEGER	false	Set based on whether 4X1GMP license is available at the SBC.	false
SIPI_ENABLED	INTEGER	false	Set based on whether Sipl license is available at the SBC.	false
SIP323_ENABLED	INTEGER	false	Set based on whether sip323 license is available at the SBC.	false
GMP1X10_ENABLED	INTEGER	false	Set based on whether 1X10GMP license is available at the SBC.	false
POLRTU_ENABLED	INTEGER	false	Set based on whether PolRtu license is available at the SBC.	false
PSXRTU_ENABLED	INTEGER	false	Set based on whether PsxRtu license is available at the SBC.	false
CAPACITY_ENABLED	INTEGER	false	Set based on whether Capacity license is available at the SBC.	false
E911_ENABLED	INTEGER	false	Set based on whether E911 license is available at the SBC.	false
ENUM_ENABLED	INTEGER	false	Set based on whether ENUM license is available at the SBC.	false
SWINSTANCE_ENABLED	INTEGER	false	Set based on whether SweInstance license is available at the SBC.	false
EVS_ENABLED	INTEGER	false	Set based on whether EVS license is available at the SBC.	false
SILK_ENABLED	INTEGER	false	Set based on whether SILK license is available at the SBC.	false

Column Name	Column Type	Index	Description	canAggregate
MEDIA_PROBE_AUTH	COUNTER	false	Set based on whether MEDIA PROBE license is available at the SBC.	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBLinkDetectionGroupStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	true	The name of the address context.	false
NAME	STRING	true	The name of this link detection group.	false
SINGLE_FAILURES	INTEGER	false	The number of single failures for this link detection group.	false
DOUBLE_FAILURES	INTEGER	false	The number of double failures for this link detection group.	false
FAILURES	INTEGER	false	The number of >2 failures for this link detection group.	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBLinkMonitorStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	true	The name of the address context.	false
GNAME	STRING	true	The name of the address context group.	false
NAME	STRING	true	The name of the link monitor.	false
MIN_TIME	INTEGER	false	The minimum time used to get a reply for an echo request packet.	false

Column Name	Column Type	Index	Description	canAggregate
MAX_TIME	INTEGER	false	The maximum time used to get a reply for an echo request packet.	false
AVERAGE_TIME	INTEGER	false	The average time used to get a reply for an echo request packet.	false
SINGLE_FAILURES	INTEGER	false	The number of single failures for this IP interface.	false
DOUBLE_FAILURES	INTEGER	false	The number of double failures for this IP interface.	false
FAILURES	INTEGER	false	The number of >2 failures for this IP interface.	false
REPLIES	INTEGER	false	The number of replies	false
DUPLICATE_REPLIES	INTEGER	false	The number of duplicate replies.	false
LATE_REPLIES	INTEGER	false	The number of late replies.	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBSipSigConnStatisticsStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	true	The name of the address context.	false
ZNAME	STRING	true	The name of the address context zone.	false
IND	GAUGE	true	The index of this SIP Signaling Port.	false
TCP_CONNECTION	COUNTER	false	Number of current TCP connections	true

Column Name	Column Type	Index	Description	canAggregate
TOTAL_TCP_CONNECTION	COUNTER	false	Number of total TCP connections made.	true
ACTIVE_TLS_TCP_CONNECTION	COUNTER	false	Number of current TLS-TCP connections made.	true
TOTAL_TLS_TCP_CONNECTION	COUNTER	false	Number of total TLS-TCP connections.	true
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBSipSigPortStatisticsStats

Column Name	Column Type	Index	Description	canAggregate
ACNAME	STRING	Yes	The name of the address context.	false
ZNAME	STRING	Yes	The name of the address context.	false
IND	GAUGE	Yes	The index of this SIP Signaling Port.	false
CALL_RATE	INTEGER	No	The number of SIP calls per second during the last minute.	true
ORIG_CALLS	INTEGER	No	Total number of outgoing calls sent out from this signaling port.	true
TERM_CALLS	INTEGER	No	Total number of incoming calls received on this signaling port.	true
TX_PDUS	COUNTER64	No	The total number of signaling PDUS sent out on this port.	true
RX_PDUS	COUNTER64	No	The total number of signaling PDUS received on this port.	true
TX_BYTES	COUNTER64	No	The total number of signaling BYTES sent out from this port.	true
RX_BYTES	COUNTER64	No	The total number of signaling BYTES received by this port.	true

Column Name	Column Type	Index	Description	canAggregate
IN_REGS	INTEGER	No	Total number of inbound registration(s) received on this signaling port.	true
OUT_REGS	INTEGER	No	Total number of outbound registration(s) sent on this signaling port.	true
TX500S	INTEGER	false	The total number of 500 responses generated by the SLB when it is unable to forward a request.	true
TX503S	INTEGER	false	The total number of 503 responses generated by the SLB when there are no backend SBCs able to handle the request due to the congestion or the cac restrictions.	true
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBSysCpuUtilIntStatsSts

Column Name	Column Type	Index	Description	canAggregate
CE_NAME	STRING	true	This object indicates the configured CE name.	false
CPU	GAUGE	true	The cpu number.	false
AVERAGE	GAUGE	false	The average cpu % utilization for this interval.	false
HIGH	GAUGE	false	The high cpu % utilization for this interval.	false
LOW	GAUGE	false	The low cpu % utilization for this interval.	false

SLBSysMemoryUtilIntStatsSts

Column Name	Column Type	Index	Description	canAggregate
CE_NAME	STRING	true	This object indicates the configured CE name.	false
AVERAGE	GAUGE	false	The average memory % utilization for this interval.	false
HIGH	GAUGE	false	The high memory % utilization for this interval.	false
LOW	GAUGE	false	The low memory % utilization for this interval.	false
AVERAGE_SWAP	GAUGE	false	The average swap memory % utilization for this interval.	false
HIGH_SWAP	GAUGE	false	The high swap memory % utilization for this interval.	false
LOW_SWAP	GAUGE	false	The low swap memory % utilization for this interval.	false

SLBSystemCongestionIntervalStats

Column Name	Column Type	Index	Description	canAggregate
NAME	INTEGER	true	A dummy key to be added to non-config scalar element container, even though only one row is allowed in container. It is because without the key, tailf treats the container non-dynamic and calls get_elem per leaf instead of calling get_object per row	false
LEVEL_MC1_COUNT	COUNTER	false	The current number of transitions into MC1	false
LEVEL_MC1_TOTAL_TIME	COUNTER	false	The current sum of time spent in MC1	false
LEVEL_MC2_COUNT	COUNTER	false	The current number of transitions into MC2	false

Column Name	Column Type	Index	Description	canAggregate
LEVEL_MC2_TOTAL_TIME	COUNTER	false	The current sum of time spent in MC2	false
LEVEL_MC3_COUNTER	COUNTER	false	The current number of transitions into MC3	false
LEVEL_MC3_TOTAL_TIME	COUNTER	false	The current sum of time spent in MC3	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBSystemLicenseInfoStats

Column Name	Type	Index	Description	canAggregate
FEATURE_NAME	STRING	true	This object indicates the feature name.	false
LICENSE_ID	STRING	true	This object indicates the license ID.	false
EXPIRATION_DATE	STRING	false	This object indicates the licence expiry date for a feature.	false
USAGE_LIMIT	INTEGER	false	This object indicates the usage limit of a feature.	true
SOURCE	STRING	false	This object indicates where the licenses is located, nodeLocked or domain.	false
IN_USE	GAUGE	false	This object indicates the number of licenses used by the application.	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SLBTcpGeneralGroupStats

Column Name	Column Type	Index	Description	canAggregate
CE_NAME	STRING	true	The name of the compute element for this entry.	false
ESTABLISHED_CONNECTIONS	GAUGE	false	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE- WAIT. (currEstab)	false
CLIENT_CONNECTIONS	COUNTER	false	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state. (activeOpens).	false
SERVER_CONNECTIONS	COUNTER	false	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state. (passiveOpens).	false
FAILED_ATTEMPTS	COUNTER	false	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state. (attemptFails)	false
IN_SEGMENTS	COUNTER	false	The total number of segments received, including those received in error. This count includes segments received on currently established connections.	false
OUT_SEGMENTS	COUNTER	false	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.	false
RETRANS_SEGMENTS	COUNTER	false	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.	false

Column Name	Column Type	Index	Description	canAggregate
IN_ERRORS	COUNTER	false	The total number of segments received in error (e.g., bad TCP checksums).	false
IN_RESETS	COUNTER	false	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state. (estabResets)	false
OUT_RESETS	COUNTER	false	The number of TCP segments sent containing the RST flag.	false

SLBUdpGeneralGroupStats

Column Name	Column Type	Index	Description	canAggregate
CE_NAME	STRING	true	The name of the compute element for this entry.	false
IN_DATAGRAMS	COUNTER	false	The total number of UDP datagrams delivered to UDP users.	false
OUT_DATAGRAMS	COUNTER	false	The total number of UDP datagrams sent from this entity.	false
UNKNOWN_PORTS	COUNTER	false	The total number of received UDP datagrams for which there was no application at the destination port.	false
IN_ERRORS	COUNTER	false	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.	false

SLBUflowOffListIntStats

Column Name	Column Type	Index	Description	canAggregate
ROLE	INTEGER	true	Role of the system.	false
SERIAL_INDEX	INTEGER	true	The index of the system	false

Column Name	Column Type	Index	Description	canAggregate
ADDRESS_CONTEXT	STRING	false	The name of the address context of the table entry	false
INTERFACE_GROUP_NAME	STRING	false	The name of the interface group of the table entry	false
INTERFACE_NAME	STRING	false	The name of the interface of the table entry	false
SOURCE_IP_ADDRESS	STRING	false	The source IP address of the table entry	false
DEST_IP_ADDRESS	STRING	false	The dest IP address of the table entry	false
SOURCE_IP_PORT	INTEGER	false	The source IP port of the table entry	false
DEST_IP_PORT	INTEGER	false	The dest IP port of the table entry	false
IP_PROTOCOL	INTEGER	false	The IP Protocol of the table entry	false
DISCARD_COUNT	COUNTER	false	The number of packets discarded by the policer	false
CE_NAME	STRING	No	The name of the compute element for this entity.	false

SBC Edge Statistics

In this section:

- [SBCEDGEChannelStatusStats](#)
- [SBCEDGENWDLLicenseStats](#)
- [SBCEDGEPTStats](#)

SBCEDGEChannelStatusStats

Column Name	Column Type	Index	Description	canAggregate
SHELF_NUMBER	GAUGE	Yes	shelf number this channel is attached to.	False
SLOT_NUMBER	GAUGE	Yes	Indicates slot number this channel is attached to.	False
PORT_NUMBER	GAUGE	Yes	Indicates port number this channel is attached to.	False
CHANNEL_NUMBER	GAUGE	Yes	Indicates (port-based) channel number this channel is attached to.	False
ADMIN_STATE	INTEGER	No	Indicates Admin state of the channel, whether administratively blocked or not.	True
OPER_STATE	INTEGER	No	Indicates all the channel states similar to the channel monitor view on Web UI.	True
IN_USE_SECONDS	COUNTER	No	Indicates the total accumulated channel connected time in seconds.	True

SBCEDGENWDLLicenseStats

Column Name	Column Type	Index	Description	canAggregate
MANAGEMENT_ID	STRING	Yes	Swelite Management Id.	False
LICENSE_NAME	STRING	Yes	Feature License Name.	False
LICENSE_USAGE	GAUGE	No	License Used.	True

SBCEDGEPTStats

Column Name	Column Type	Index	Description	canAggregate
INDEX_PT	GAUGE	Yes	Indicates Index for the port table.	False

Column Name	Column Type	Index	Description	canAggregate
SHELF	GAUGE	No	Indicates the shelf number this port is assigned to.	True
SLOT	GAUGE	No	Indicates the (slot-based) port this port is assigned to.	True
PORT	GAUGE	No	Indicates the (slot-based) port this port is assigned to.	True
CURRENT_CALLS	GAUGE	No	Indicates the Current number of active managed calls on this server.	True
TOTAL_CALLS	GAUGE	No	Indicates the Current number of stable managed calls on this server.	True
CONNECTED_CALLS	COUNTER	No	Indicates the number of calls answered on this port.	True
REFUSED_CALLS	COUNTER	No	Indicates the number of calls refused on this port.	True
ERRORED_CALLS	COUNTER	No	Indicates the number of errors on this port.	True
EGRESS_CALL_ATTEMPTS	COUNTER	No	Indicates the total number of Egress call attempts on this port	True
EGRESS_CALLS_ACCEPTED	COUNTER	No	Indicates the number of Egress successful call attempts on this port.	True
EGRESS_CALLS_COMPLETED	COUNTER	No	Indicates the number of successfully completed Egress calls on this port.	True
EGRESS_CALLS_REJECTED	COUNTER	No	Indicates the number of Egress calls from this port that were rejected.	True
INGRESS_CALL_ATTEMPTS	COUNTER	No	Indicates the total number of Ingress call attempts on this port.	True

Column Name	Column Type	Index	Description	canAggregate
INGRESS_CALLS_ACCEPTED	COUNTER	No	Indicates the total number of Ingress calls accepted on this port.	True
INGRESS_CALLS_COMPLETED	COUNTER	No	Indicates the number of successfully completed Ingress calls on this port.	True
INGRESS_CALLS_REJECTED	COUNTER	No	Indicates the number of Ingress calls to this port that were rejected.	True
BLOCKED_CALLS	COUNTER	No	Indicates number of calls blocked per channel per port.	True
EGRESS_BLOCKED_CALLS	COUNTER	No	Indicates number of Egress calls blocked on this port.	True
INGRESS_BLOCKED_CALLS	COUNTER	No	Indicates number of Ingress calls blocked on this port.	True
EGRESS_CURRENT_CALLS	COUNTER	No	Indicates number of Egress active calls on this port.	True
INGRESS_CURRENT_CALLS	COUNTER	No	Indicates number of Ingress active calls on this port.	True
BHCCARATE	COUNTER	No	Indicates BHCA rate per DS1.	True
BHCCRATE	COUNTER	No	Indicates BHCC rate per DS1.	True

SGX4000 Statistics

In this section:

- [SGX4000M2paM2paLinkAvailStats](#)
- [SGX4000M2paM2paLinkMeasStats](#)
- [SGX4000M3uaAspLinkAvailStats](#)
- [SGX4000M3uaAspLinkMeasureStats](#)
- [SGX4000M3uaSgpLinkAvailStats](#)
- [SGX4000M3uaSgpLinkMeasureStats](#)
- [SGX4000Ss7Mtp2LinkAvailStats](#)
- [SGX4000Ss7Mtp2LinkMeasStats](#)
- [SGX4000Ss7SccpErrorStats](#)
- [SGX4000Ss7T1E1TrunkStats](#)

- [SGX4000SuaSgpLinkAvailStats](#)
- [SGX4000SuaSgpLinkMeasureStats](#)
- [SGX4000SystemCPUUtilStats](#)
- [SGX4000SystemMemoryUtilStats](#)

SGX4000M2paM2paLinkAvailStats

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
LINK_NAME	STRING	Yes	The existing M2PA link name.
DUR_IN_ISSTATE	GAUGE	No	The time duration for which link was in inService status.
DUR_UN_AVAILABLE	GAUGE	No	The time duration for which link was unavailable.
DUR_UN_AVAILABLE_RSN_FAIL	GAUGE	No	The time duration for which link was unavailable due to link failure.
DUR_OF_LOCAL_LINK_BUSY	GAUGE	No	The time duration for which link was locally busy.
NUM_OF_ALIGN_OR_PROVIDE_FAIL	GAUGE	No	The number of link alignment OR proving failure.
NUM_OF_SIG_UNIT_RECEIVED_IN_ERR	GAUGE	No	The number of signal units received in error.
NUM_OF_LINK_FAILURES	GAUGE	No	The number of link failures.

SGX4000M2paM2paLinkMeasStats

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
LINK_NAME	STRING	Yes	The existing M2PA link name.
SIF_TRANSMITTED	GAUGE	No	The number of SIF messages transmitted.

Column Name	Column Type	Index	Description
SIF_RECEIVED	GAUGE	No	The number of SIF messages received.
SIO_TRANSMITTED	GAUGE	No	The number of SIO messages transmitted.
SIO_RECEIVED	GAUGE	No	The number of SIO messages received.
MSU_TRANSMITTED	GAUGE	No	The number of MSUs transmitted.
MSU_RECEIVED	GAUGE	No	The number of MSUs received.
NUM_OF_LOCAL_CONG_IND	GAUGE	No	The number of local congestion indications received.
CUM_DUR_OF_LINK_CONG	GAUGE	No	The cumulative time duration for which link was in congestion status
MSU_DISCARDED_RSN_CONG	GAUGE	No	The number of MSUs discarded due to link level congestion.
NUM_OF_CONG_RESULT_LOSS_MSU	GAUGE	No	The number of times the link was congested leading to MSU loss.
ISUP_MSG_TRANSMITTED	GAUGE	No	The number of ISUP messages transmitted.
ISUP_MSG_RECEIVED	GAUGE	No	The number of ISUP messages received.
SCCP_MSG_TRANSMITTED	GAUGE	No	The number of SCCP messages transmitted.
SCCP_MSG_RECEIVED	GAUGE	No	The number of SCCP messages received.
ISUP_OCTETS_TRANSMITTED	GAUGE	No	The number of ISUP octets transmitted.
ISUP_OCTETS_RECEIVED	GAUGE	No	The number of ISUP octets received.
SCCP_OCTETS_TRANSMITTED	GAUGE	No	The number of SCCP octets transmitted.

Column Name	Column Type	Index	Description
SCCP_OCTETS_RECEIVED	GAUGE	No	The number of SCCP octets received.

SGX4000M3uaAspLinkAvailStats

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
LINK_NAME	STRING	Yes	The existing M3UA ASP link name.
TIME_LINK_UP	GAUGE	No	The time duration for which link was in ASP UP status.
TIME_LINK_DOWN	GAUGE	No	The time duration for which link was unavailable.
TIME_LINK_DOWN_REASON_FAIL	GAUGE	No	The time duration for which link was unavailable due to link failure.
NUM_LINK_FAILURES	GAUGE	No	The number of link failures.

SGX4000M3uaAspLinkMeasureStats

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
LINK_NAME	STRING	Yes	The existing M3UA ASP link name.
ASP_ACTIVE_RECVD	COUNTER	No	The number of ASP ACTIVE messages received.
ASP_ACTIVE_XMIT	COUNTER	No	The number of ASP ACTIVE messages transmitted.
ASP_ACTIVE_ACK_RECVD	COUNTER	No	The number of ASP ACTIVE ACK messages received.
ASP_ACTIVE_ACK_XMIT	COUNTER	No	The number of ASP ACTIVE ACK messages transmitted.

Column Name	Column Type	Index	Description
ASP_DOWN_RECVD	COUNTER	No	The number of ASP DOWN messages received.
ASP_DOWN_XMIT	COUNTER	No	The number of ASP DOWN messages transmitted.
ASP_DOWN_ACK_RECVD	COUNTER	No	The number of ASP DOWN ACK messages received.
ASP_DOWN_ACK_XMIT	COUNTER	No	The number of ASP DOWN ACK messages transmitted.
ASP_IN_ACTIVE_RECVD	GAUGE	No	The number of ASP INACTIVE messages received.
ASP_IN_ACTIVE_XMIT	GAUGE	No	The number of ASP INACTIVE messages transmitted.
ASP_IN_ACTIVE_ACK_RECVD	GAUGE	No	The number of ASP INACTIVE ACK messages received.
ASP_IN_ACTIVE_ACK_XMIT	GAUGE	No	The number of ASP INACTIVE ACK messages transmitted.
ASP_UP_RECVD	COUNTER	No	The number of ASP UP messages received.
ASP_UP_XMIT	COUNTER	No	The number of ASP UP messages transmitted.
ASP_UP_ACK_RECVD	COUNTER	No	The number of ASP UP ACK messages received.
ASP_UP_ACK_XMIT	COUNTER	No	The number of ASP UP ACK messages transmitted.
BEAT_RECVD	COUNTER	No	The number of BEAT messages received.
BEAT_XMIT	COUNTER	No	The number of BEAT messages transmitted.
BEAT_ACK_RECVD	COUNTER	No	The number of BEAT ACK messages received.

Column Name	Column Type	Index	Description
BEAT_ACK_XMIT	COUNTER	No	The number of BEAT ACK messages transmitted.
DATA_RECVD	COUNTER	No	The number of DATA messages received.
DATA_XMIT	COUNTER	No	The number of DATA messages transmitted.
DAUD_RECVD	COUNTER	No	The number of DAUD messages received.
DAUD_XMIT	COUNTER	No	The number of DAUD messages transmitted.
DAVA_RECVD	COUNTER	No	The number of DAVA messages received.
DAVA_XMIT	COUNTER	No	The number of DAVA messages transmitted.
DEREG_REQUEST_RECV D	GAUGE	No	The number of DEREG REQ messages received.
DEREG_REQUEST_XMIT	GAUGE	No	The number of DEREG REQ messages transmitted.
DEREG_RESPONSE_RECV D	GAUGE	No	The number of DEREG RSP messages received.
DEREG_RESPONSE_XMIT	GAUGE	No	The number of DEREG RSP messages transmitted.
DUNA_RECVD	COUNTER	No	The number of DUNA messages received.
DUNA_XMIT	COUNTER	No	The number of DUNA messages transmitted.
DUPU_RECVD	COUNTER	No	The number of DUPU messages received.
DUPU_XMIT	COUNTER	No	The number of DUPU messages transmitted.

Column Name	Column Type	Index	Description
ERROR_MSG_RECVD	GAUGE	No	The number of ERR messages received.
ERROR_MSG_XMIT	GAUGE	No	The number of ERR messages transmitted.
NOTIFY_MSG_RECVD	GAUGE	No	The number of NOTIFY messages received.
NOTIFY_MSG_XMIT	GAUGE	No	The number of NOTIFY messages transmitted.
REG_REQUEST_RECVD	GAUGE	No	The number of REG REQ messages received.
REG_REQUEST_XMIT	GAUGE	No	The number of REG REQ messages transmitted.
REG_RESPONSE_RECVD	GAUGE	No	The number of REG RSP messages received.
REG_RESPONSE_XMIT	GAUGE	No	The number of REG RSP messages transmitted.
SCON_RECVD	COUNTER	No	The number of SCON messages received.
SCON_XMIT	COUNTER	No	The number of SCON messages transmitted.
INVALID_MSG_RECVD	GAUGE	No	The number of invalid messages received.
UNRECOGNIZED_MSG_RECVD	GAUGE	No	The number of unrecognized messages received.

SGX4000M3uaSgpLinkAvailStats

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
LINK_NAME	STRING	Yes	The existing M3UA SGP link name.

Column Name	Column Type	Index	Description
TIME_LINK_UP	GAUGE	No	The time duration for which link was in ASP UP status.
TIME_LINK_DOWN	GAUGE	No	The time duration for which link was unavailable.
TIME_LINK_DOWN_REASON_FAIL	GAUGE	No	The time duration for which link was unavailable due to link failure.
NUM_LINK_FAILURES	GAUGE	No	The number of link failures.

SGX4000M3uaSgpLinkMeasureStats

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
LINK_NAME	STRING	Yes	The existing M3UA SGP link name.
ASP_ACTIVE_RECVD	COUNTER	No	The number of ASP ACTIVE messages received.
ASP_ACTIVE_XMIT	COUNTER	No	The number of ASP ACTIVE messages transmitted.
ASP_ACTIVE_ACK_RECVD	COUNTER	No	The number of ASP ACTIVE ACK messages received.
ASP_ACTIVE_ACK_XMIT	COUNTER	No	The number of ASP ACTIVE ACK messages transmitted.
ASP_DN_RECVD	COUNTER	No	The number of ASP DOWN messages received.
ASP_DN_XMIT	COUNTER	No	The number of ASP DOWN messages transmitted.
ASP_DN_ACK_RECVD	COUNTER	No	The number of ASP DOWN ACK messages received.
ASP_DN_ACK_XMIT	COUNTER	No	The number of ASP DOWN ACK messages transmitted.

Column Name	Column Type	Index	Description
ASP_IN_ACTIVE_RECVD	GAUGE	No	The number of ASP INACTIVE messages received.
ASP_IN_ACTIVE_XMIT	GAUGE	No	The number of ASP INACTIVE messages transmitted.
ASP_IN_ACTIVE_ACK_RECVD	GAUGE	No	The number of ASP INACTIVE ACK messages received.
ASP_IN_ACTIVE_ACK_XMIT	GAUGE	No	The number of ASP INACTIVE ACK messages transmitted.
ASP_UP_RECVD	COUNTER	No	The number of ASP UP messages received.
ASP_UP_XMIT	COUNTER	No	The number of ASP UP messages transmitted.
ASP_UP_ACK_RECVD	COUNTER	No	The number of ASP UP ACK messages received.
ASP_UP_ACK_XMIT	COUNTER	No	The number of ASP UP ACK messages transmitted.
BEAT_RECVD	COUNTER	No	The number of BEAT messages received.
BEAT_XMIT	COUNTER	No	The number of BEAT messages transmitted.
BEAT_ACK_RECVD	COUNTER	No	The number of BEAT ACK messages received.
BEAT_ACK_XMIT	COUNTER	No	The number of BEAT ACK messages transmitted.
DATA_RECVD	COUNTER	No	The number of DATA messages received.
DATA_XMIT	COUNTER	No	The number of DATA messages transmitted.
DAUD_RECVD	COUNTER	No	The number of DAUD messages received.

Column Name	Column Type	Index	Description
DAUD_XMIT	COUNTER	No	The number of DAUD messages transmitted.
DAVA_RECVD	COUNTER	No	The number of DAVA messages received.
DAVA_XMIT	COUNTER	No	The number of DAVA messages transmitted.
DEREG_REQUEST_RECVD	GAUGE	No	The number of DEREG REQ messages received.
DEREG_REQUEST_XMIT	GAUGE	No	The number of DEREG REQ messages transmitted.
DEREG_RESPONSE_RECVD	GAUGE	No	The number of DEREG RSP messages received.
DEREG_RESPONSE_XMIT	GAUGE	No	The number of DEREG RSP messages transmitted.
DUNA_RECVD	COUNTER	No	The number of DUNA messages received.
DUNA_XMIT	COUNTER	No	The number of DUNA messages transmitted.
DUPU_RECVD	COUNTER	No	The number of DUPU messages received.
DUPU_XMIT	COUNTER	No	The number of DUPU messages transmitted.
ERROR_MSG_RECVD	GAUGE	No	The number of ERR messages received.
ERROR_MSG_XMIT	GAUGE	No	The number of ERR messages transmitted.
NOTIFY_MSG_RECVD	GAUGE	No	The number of NOTIFY messages received.
NOTIFY_MSG_XMIT	GAUGE	No	The number of NOTIFY messages transmitted.

Column Name	Column Type	Index	Description
REG_REQUEST_RECVD	GAUGE	No	The number of REG REQ messages received.
REG_REQUEST_XMIT	GAUGE	No	The number of REG REQ messages transmitted.
REG_RESPONSE_RECVD	GAUGE	No	The number of REG RSP messages received.
REG_RESPONSE_XMIT	GAUGE	No	The number of REG RSP messages transmitted.
SCON_RECVD	COUNTER	No	The number of SCON messages received.
SCON_XMIT	COUNTER	No	The number of SCON messages transmitted.
INVALID_MSG_RECVD	GAUGE	No	The number of invalid messages received.
UNRECOGNIZED_MSG_RECVD	GAUGE	No	The number of unrecognized messages received.

SGX4000Ss7Mtp2LinkAvailStats

Note

The minimum collection interval configured on SGX4000 can be 15 minutes.

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
LINK_NAME	STRING	Yes	The existingMTP2 link name.
DUR_IN_ISSTATE	GAUGE	No	The time duration for which link was in inService status.
DUR_UN_AVAILABLE	GAUGE	No	The time duration for which link was unavailable.

Column Name	Column Type	Index	Description
DUR_UN_AVAILABLE_RSN_FAIL	GAUGE	No	The time duration for which link was unavailable due to link failure.
DUR_OF_LOCAL_LINK_BUSY	GAUGE	No	The time duration for which link was locally busy.
NUM_OF_ALIGN_OR_PROVING_FAIL	GAUGE	No	The number of link alignment OR proving failure.
NUM_OF_SIG_UNIT_RECEIVED_IN_ERR	GAUGE	No	The number of signal units received in error.
NUM_OF_NEGATIVE_ACKS	GAUGE	No	The number of negative Acknowledgement.
NUM_OF_LINK_FAILURES	GAUGE	No	The number of link failures.

SGX4000Ss7Mtp2LinkMeasStats

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
LINK_NAME	STRING	Yes	The existing MTP2 link name.
SIF_AND_SIO_TRANSMITTED	GAUGE	No	The number of SIF and SIO messages transmitted.
SIF_AND_SIO_RECEIVED	GAUGE	No	The number of SIF and SIO messages received.
NUM_OF_OCTETS_RE_TRANSMITTED	GAUGE	No	The number of octets re-transmitted.
MSU_TRANSMITTED	GAUGE	No	The number of MSUs transmitted.
MSU_RECEIVED	GAUGE	No	The number of MSUs received.
NUM_OF_LOCAL_CONGESTION_IND	GAUGE	No	The number of local congestion indications received.

Column Name	Column Type	Index	Description
CUM_DUR_OF_LINK_CONG	GAUGE	No	The cumulative time duration for which link was in congestion status.
NUM_OF_CONG_RESULT_LOSSOF_MSU	GAUGE	No	The number of times the link was congested leading to MSU loss.
ISUP_MSG_TRANSMITTED	GAUGE	No	The number of ISUP messages transmitted.
ISUP_MSG_RECEIVED	GAUGE	No	The number of ISUP messages received.
SCCP_MSG_TRANSMITTED	GAUGE	No	The number of SCCP messages transmitted.
SCCP_MSG_RECEIVED	GAUGE	No	The number of SCCP messages received.
ISUP_OCTETS_TRANSMITTED	GAUGE	No	The number of ISUP octets transmitted.
ISUP_OCTETS_RECEIVED	GAUGE	No	The number of ISUP octets received.
SCCP_OCTETS_TRANSMITTED	GAUGE	No	The number of SCCP octets transmitted.
SCCP_OCTETS_RECEIVED	GAUGE	No	The number of SCCP octets received.
SIF_OCTETS_RECEIVED	GAUGE	No	The number of SIF octets received.
SIF_OCTETS_TRANSMITTED	GAUGE	No	The number of SIF octets transmitted.
SIO_OCTETS_RECEIVED	GAUGE	No	The number of SIO octets received.
SIO_OCTETS_TRANSMITTED	GAUGE	No	The number of SIO octets transmitted.
NUM_OF_REMOTE_CONG_IND	GAUGE	No	The number of remote congestion indications received.
NUM_OF_LOCAL_OUTAGE_IND	GAUGE	No	The number of local outage indications received.

Column Name	Column Type	Index	Description
NUM_OF_REMOTE_OUTAGE_IND	GAUGE	No	The number of remote outage indications received.
SIGNALING_LINK_FAILURES_ALL	GAUGE	No	The number of signaling link failure for all reasons.

SGX4000Ss7SccpErrorStats

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
HOP_COUNTER_VIOLATION	COUNTER	No	The number of hop counter violation over the given period of time interval.
MSG_RECVD_SYNTAX_ERROR	COUNTER	No	The number of messages received with syntax error.
MSG_TOO_LARGE_FOR_SEGMENT	COUNTER	No	The number of messages that were too large for segmentation.
ROUTEFAIL_NET_CONGESTION	GAUGE	No	The number of routing failures due to network congestion.
ROUTEFAIL_NO_GTT_ADDR_NATURE	GAUGE	No	The number of routing failures due to unavailable GTT for address of such nature.
ROUTEFAIL_NO_GTT_SPECI_ADDR	GAUGE	No	The number of routing failures due to unavailable GTT for this specific address.
ROUTEFAIL_SS7_DEST_UNAVAIL	GAUGE	No	The number of routing failures due to unavailable SS7 destination.
ROUTEFAIL_SUBSYS_UNAVAIL	GAUGE	No	The number of routing failures due to unavailability of SCCP sub system.
ROUTEFAIL_SUBSYS_CONGESTION	GAUGE	No	The number of routing failures due to congestion at SCCP sub system
ROUTEFAIL_SUBSYS_UNEQUIPPED	GAUGE	No	The number of routing failures due to unequipped SCCP sub System.

Column Name	Column Type	Index	Description
ROUTEFAIL_UNQUALI_US ER	GAUGE	No	The number of routing failures due to unqualified SCCP user.
REASSEM_ERR_NO_SPAC E	GAUGE	No	The number of reassembly errors due to unavailability of reassembling space.
REASSEM_ERR_TIMER_E XPIRY	GAUGE	No	The number of reassembly errors due to reassembly timer expiry.
REASSEM_ERR_FAILED	GAUGE	No	The number of reassembly errors due to reassembly failure.
REASSEM_ERR_SEGMEN T_OOS	GAUGE	No	The number of reassembly errors due to receipt of segmented message out of sequence.
SEG_ERROR_FAILED	GAUGE	No	The number of segmentation errors due to segmentation failure.

SGX4000Ss7T1E1TrunkStats

Note

The minimum collection interval configured on SGX4000 can be 15 minutes.

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
TRUNK_NAME	STRING	Yes	The existing T1/E1 trunk name.
BIPOLAR_VIOLATIONS	GAUGE	No	This gives the count of bipolar violations.
CRC_ERRORS	GAUGE	No	This gives the count of CRC errors.
FRAME_SLIPS	GAUGE	No	This gives the count of frame slips.
ALIGNMENT_ERRS	GAUGE	No	This gives the count of alignment errors.

Column Name	Column Type	Index	Description
ERRS_PER_SEC	GAUGE	No	This gives the number of times any anomaly events occurred such as CRC, Frame Slip in one second time period.
SEVERE_ERRS_PER_SEC	GAUGE	No	This gives the number of times any severe errors occurred such as RED alarm, yellow alarm in one second time period.
UNAVAIL_SECS	GAUGE	No	This gives the number of seconds the trunk was unavailable
SEVERELY_ERRORED_FRAMING_SEC	GAUGE	No	This gives the number of Severely Errored Framing Seconds.
CONTROLLED_SLIP_SECONDS	GAUGE	No	This gives the number of Controlled Slip Seconds.
PATH_CODE_VIOLATIONS	GAUGE	No	This gives the number of Path Code Violations
LINE_ERRORED_SECONDS	GAUGE	No	This gives the number of Line Errored Seconds.
BURSTY_ERRORED_SECONDS	GAUGE	No	This gives the number of Bursty Errored Seconds
DEGRADED_MINUTES	GAUGE	No	This gives the number of Degraded Minutes.
LINE_CODING_VIOLATIONS	GAUGE	No	This gives the number of Line Coding Violations

Note

The columns BIPOLAR_VIOLATIONS, CRC_ERRORS, FRAME_SLIPS, and ALIGNMENT_ERRS are not supported.

SGX4000SuaSgpLinkAvailStats

Note

The minimum collection interval configured on SGX4000 can be 15 minutes.

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
LINK_NAME	STRING	Yes	The existing SUA SGP link name.
TIME_LINK_UP	GAUGE	No	The time duration for which link was in ASP UP status.
TIME_LINK_DOWN	GAUGE	No	The time duration for which link was unavailable.
TIME_LINK_DOWN_REASON_FAIL	GAUGE	No	The time duration for which link was unavailable due to link failure.
NUM_LINK_FAILURES	GAUGE	No	The number of link failures.

SGX4000SuaSgpLinkMeasureStats

Note

The minimum collection interval configured on SGX4000 can be 15 minutes.

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
LINK_NAME	STRING	Yes	The existing SUA SGP link name.
ASP_ACTIVE_RECVD	GAUGE	No	The number of ASP ACTIVE messages received.

Column Name	Column Type	Index	Description
ASP_ACTIVE_XMIT	GAUGE	No	The number of ASP ACTIVE messages transmitted.
ASP_ACTIVE_ACK_RECVD	GAUGE	No	The number of ASP ACTIVE ACK messages received.
ASP_ACTIVE_ACK_XMIT	GAUGE	No	The number of ASP ACTIVE ACK messages transmitted.
ASP_DOWN_RECVD	GAUGE	No	The number of ASP DOWN messages received.
ASP_DOWN_XMIT	GAUGE	No	The number of ASP DOWN messages transmitted.
ASP_DOWN_ACK_RECVD	GAUGE	No	The number of ASP DOWN ACK messages received.
ASP_DOWN_ACK_XMIT	GAUGE	No	The number of ASP DOWN ACK messages transmitted.
ASP_IN_ACTIVE_RECVD	GAUGE	No	The number of ASP INACTIVE messages received.
ASP_IN_ACTIVE_XMIT	GAUGE	No	The number of ASP INACTIVE messages transmitted.
ASP_IN_ACTIVE_ACK_RECVD	GAUGE	No	The number of ASP INACTIVE ACK messages received.
ASP_IN_ACTIVE_ACK_XMIT	GAUGE	No	The number of ASP INACTIVE ACK messages transmitted.
ASP_UP_RECVD	GAUGE	No	The number of ASP UP messages received.
ASP_UP_XMIT	GAUGE	No	The number of ASP UP messages transmitted.
ASP_UP_ACK_RECVD	GAUGE	No	The number of ASP UP ACK messages received.
ASP_UP_ACK_XMIT	GAUGE	No	The number of ASP UP ACK messages transmitted.

Column Name	Column Type	Index	Description
BEAT_RECVD	GAUGE	No	The number of BEAT messages received.
BEAT_XMIT	GAUGE	No	The number of BEAT messages transmitted.
BEAT_ACK_RECVD	GAUGE	No	The number of BEAT ACK messages received.
BEAT_ACK_XMIT	GAUGE	No	The number of BEAT ACK messages transmitted.
CLDR_RECVD	GAUGE	No	The number of CLDR messages received.
CLDR_XMIT	GAUGE	No	The number of CLDR messages transmitted.
CLDT_RECVD	GAUGE	No	The number of CLDT messages received.
CLDT_XMIT	GAUGE	No	The number of CLDT messages transmitted.
DAUD_RECVD	GAUGE	No	The number of DAUD messages received.
DAUD_XMIT	GAUGE	No	The number of DAUD messages transmitted.
DAVA_RECVD	GAUGE	No	The number of DAVA messages received.
DAVA_XMIT	GAUGE	No	The number of DAVA messages transmitted.
DEREG_REQUEST_RECV D	GAUGE	No	The number of DEREG REQ messages received.
DEREG_REQUEST_XMIT	GAUGE	No	The number of DEREG REQ messages transmitted.
DEREG_RESPONSE_RECV VD	GAUGE	No	The number of DEREG RSP messages received.

Column Name	Column Type	Index	Description
DEREG_RESPONSE_XMIT	GAUGE	No	The number of DEREG RSP messages transmitted.
DUNA_RECVD	GAUGE	No	The number of DUNA messages received.
DUNA_XMIT	GAUGE	No	The number of DUNA messages transmitted.
DUPU_RECVD	GAUGE	No	The number of DUPU messages received.
DUPU_XMIT	GAUGE	No	The number of DUPU messages transmitted.
ERROR_MESSAGES_RECV VD	GAUGE	No	The number of ERR messages received.
ERROR_MESSAGES_XMIT	GAUGE	No	The number of ERR messages transmitted.
NOTIFY_MESSAGES_RECV VD	GAUGE	No	The number of NOTIFY messages received.
NOTIFY_MESSAGES_XMIT	GAUGE	No	The number of NOTIFY messages transmitted.
REG_REQUEST_RECVD	GAUGE	No	The number of REG REQ messages received.
REG_REQUEST_XMIT	GAUGE	No	The number of REG REQ messages transmitted.
REG_RESPONSE_RECVD	GAUGE	No	The number of REG RSP messages received.
REG_RESPONSE_XMIT	GAUGE	No	The number of REG RSP messages transmitted.
SCON_RECVD	GAUGE	No	The number of SCON messages received.
SCON_XMIT	GAUGE	No	The number of SCON messages transmitted.

Column Name	Column Type	Index	Description
INVALID_MSG_RECVD	GAUGE	No	The number of invalid messages received.
UNRECOGNIZED_MSG_RE CVD	GAUGE	No	The number of unrecognized messages received.

SGX4000SystemCPUUtilStats

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
CPU	GAUGE	No	The CPU number.
AVERAGE	GAUGE	No	The average CPU % utilization for this interval.
HIGH	GAUGE	No	The high CPU % utilization for this interval.
LOW	GAUGE	No	The low CPU % utilization for this interval

SGX4000SystemMemoryUtilStats

Column Name	Column Type	Index	Description
CE_NAME	STRING	Yes	This object indicates the configured CE name.
AVERAGE	GAUGE	No	The average memory % utilization for this interval.
HIGH	GAUGE	No	The high memory % utilization for this interval.
LOW	GAUGE	No	The low memory % utilization for this interval.
AVERAGE_SWAP	GAUGE	No	The average swap % memory utilization for this interval.

Column Name	Column Type	Index	Description
HIGH_SWAP	GAUGE	No	The high swap % memory utilization for this interval.
LOW_SWAP	GAUGE	No	The low swap % memory utilization for this interval.

RAMP System Configuration

In this section:

- [System Registration](#)
- [Application Configuration](#)
- [Change IP Address](#)
- [System Activity Logging](#)
- [Exporting Logs to a Remote Syslog Server](#)
- [Device REST Credentials](#)
- [SSH Active Channels](#)
- [RAMP Profile Settings](#)
- [Database Configuration](#)
- [PSX Call Trace Destination](#)
- [PSX Manager Version Compatibility](#)
- [GSX User Interface](#)
 - [Restrict Access to GSX Commands](#)
 - [Configuration Files for GSX Navigator and Task Configurator](#)
 - [Set GSX Navigator Discovery](#)
 - [Sort GSX Trunk Groups](#)
- [SSH Configuration](#)

Use the windows under **System** to configure options and use controls that manage the Ribbon Application Management Platform (RAMP) system.

System Registration

Note

This window is not available unless the EdgeView (EV) service is installed and running on RAMP.

Use the **System Registration** window to enter registration credentials if your Ribbon Application Management Platform (RAMP) deployment manages SBC SWe Edge devices. The credentials consist of a registration key and password provided by Ribbon during the sales process, along with the email address associated with that transaction. You must enter this information for RAMP to validate the SBC Edge device's Management ID during registered.

Use the following procedure to access the **System Registration** window and enter RAMP registration credentials.

Note

System registration credentials are not applicable to SBC 1000/2000 and Edge 8000.

Note

The system registration is also required if RAMP deployment manages EdgeMarc devices to support auto provisioning of EdgeMarc.

Prerequisites

Registration credentials from Ribbon to enable managing SBC Edge devices with RAMP. Contact your Ribbon representative to obtain registration credentials.

Start

1. Log on to the RAMP GUI.
2. Navigate to **System > System Registration**.
3. In **Email Address**, enter the email associated with the RAMP registration credentials.
4. In **Key** and **Password**, enter the registration key and registration password that Ribbon provided.
5. Click **Register**.

Application Configuration

Note

The RAMP will continue to include EMS-labeled parameters and screens to facilitate the SBC migrations from older releases. Accordingly, any references to "EMS" in this documentation pertains to the RAMP platform.

Use the **Application Config** window to configure parameters for different processes and applications running on the Ribbon Application Management Platform (RAMP).

Use the following procedure to access the **Application Config** window [and configure parameters for one or more components](#):

Start

1. Log on to the RAMP GUI.
2. Navigate to **System > Application Config**.
3. In **Devices**, click the name of your RAMP system. The **Components** list is populated.
4. Click on a name in the **Components** list to open an area with the configurable parameters for that specific component.
5. Enter or select values for the parameters using the tables below.
6. Click **Apply**.
7. Select additional components until you have reviewed all of the parameters and made any necessary changes.

Links to Parameter Tables:

- [Agent Parameters](#)
- [Call Analysis Parameters](#)
- [Cluster Parameters](#)
- [EMS API Parameters](#)
- [Entity Manager Parameters](#)
- [GSX Upgrade Parameters](#)
- [Hornet Management Parameters](#)
- [Hornet Management Ext Parameters](#)
- [List All Parameters](#)
- [LNP Adaptor Parameters](#)
- [MNP Services Parameters](#)
- [NHR Parameters](#)
- [Node Admin Parameters](#)
- [PSX CLI Parameters](#)
- [RADIUS Parameters](#)
- [Report Framework Parameters](#)
- [SBC GUI Parameters](#)
- [SGX API Parameters](#)
- [SBC API Parameters](#)
- [SBC Management Parameters](#)
- [Telnet Session Manager Parameters](#)
- [Trunkgroup Validator Parameters](#)
- [UI Gen Parameters](#)
- [Utilities Parameters](#)

Agent Parameters

Parameter	Description
Use FTPS for Agent FTP	Specifies whether to use FTPS (FTP over SSL/TLS) when making an FTP connection to a device agent. The default value is True.

Call Analysis Parameters

Parameter	Description
Purger Task Frequency	Specifies how often the system runs the Purger task to remove old call trace files. • Every day (default) • Every 2 days • Every week
Purger Task Start Time	Specifies when to start running the Purger task. Subsequent times are determined by Purger Task Frequency . Use the format: (day of week:hh:mm:AM / PM). For example, Fri:02:30:PM. The default value is Sun:05:00:AM.

Parameter	Description
Call Trace Retention Period	Specifies the interval of call trace data that the system retains in the database. • None • 1 day • 2 days (default) • 1 week • 2 weeks • 3 weeks • 4 weeks

Cluster Parameters

Parameter	Description
The max polling count for configuration push status check	Specifies the maximum number of times to poll for status (at 30 seconds intervals), after pushing a configuration to a device, before the push is declared as timed out. The default value is 120.
Retention period (in minutes) for Configuration push context file	Specifies the amount of time (in minutes) before an unused configuration push context file created is deleted. Range: 15 to 45. The default value is 30 minutes.
The time (in min) before a trap is generated to indicate an SBC Core head end has been used to update the cluster configuration but not yet activate it	Specifies the amount of time (in minutes) before a <code>sonusEmsClusterConfigHeadendOutofsyncNotification</code> trap is sent out if the SBC Core Headend has been updating a cluster configuration but has not yet activated it. Range is 10 to 1440. The default value is 60 minutes.
Cluster configuration limit enabled	Specifies whether setting a limit on the number of configurations on a cluster is enabled. • False • True (default)
The max number of cluster configurations stored	Specifies a limit on the number of cluster configurations to store. When the limit is reached, older configurations are deleted. range is 1 to 200. The default value is 50.

Parameter	Description
Rate-Limit on API request enabled	Specifies whether to enable basic rate-limiting on cluster management API requests. This rate-limit applies only to the cluster configuration download API. • False (default) • True
Rate-limit maximum number of allowed permits	Specifies the maximum number of concurrent permits/requests allowed. • 5 (default) • 10 • 15 • 25 • 50
Rate-limit wait time duration	Specifies the interval to wait (in seconds) for each permit to become available again after it is acquired by a previous request. • 10 (default) • 20 • 30 • 40 • 50 • 60

EMS API Parameters

Parameter	Description
Deploy PSX version 7.1.0 to Deploy PSX version 8.4.14	Specifies whether to to deploy the RAMP PSX API (on a per version basis). • False (default) • True
Deploy PSX version 9.0.0 to Deploy PSX version 14.1.0	Specifies whether to to deploy the RAMP PSX API (on a per version basis). • False • True (default)
Maximum batch size	Specifies the maximum allowable batch size when using batch operations. The default value is "Max batch size = 500".

Parameter	Description
Operations Logging Level	Specifies how much information is logging for each operation. • NORMAL – (Default) Each operation is logged. • OFF – No information is logged. • Entity level details are logged. Note that VERBOSE logging may impact performance.

Note

Ribbon recommends to deploy only the RAMP PSX API for the versions in use. Use of the API capabilities also requires the presence of the appropriate license.

Entity Manager Parameters

Parameter	Description
Connection Timeout	Specifies the timeout (in seconds) for initial socket connection to PSX. The default value is 10 seconds.
Read Timeout	Specifies the timeout (in seconds) for socket read from PSX. The maximum value allowed is 1800 seconds. The default value is 60 seconds.

GSX Upgrade Parameters

Parameter	Description
NFS Disk Space Minimum	Specifies the minimum amount of free disk space (in megabytes) required on the NFS before allowing a software copy operation to the NFS. Range: 200-10,000 MB. The default value is 1000 MB.
Local Disk Space Minimum	Specifies the minimum amount of free disk space (in megabytes) required on the local file system before allowing import operations. Range: 200-10,000 MB. The default value is 1000 MB.
Tasks Per Job	Specifies the maximum number of simultaneous GSXs allowed with an 'In Progress' status, per Job. Range: 1-4 GSXs per Job. The default value is 4.

Parameter	Description
Total Tasks	Specifies the maximum number of simultaneous GSXs allowed with an 'In Progress' status, per RAMP (across all Jobs). Range: 1-16 tasks. The default value is 16.
Audit Log Purger Task Frequency	Specifies how often the system runs the data Purger that removes old audit logs from the database. • Every week (default) • Every 4 weeks
Audit Log Purger Task Start Time	Specifies how often to run the data Purger task. Subsequent times are determined by Purger Task Frequency. Use the format: (Day of week:hh:mm:AM / PM). For example, Fri:02:30:PM. The default value is Sun:02:00:AM.
Audit Log Retention Period	Specifies the interval to retain audit logs in the database. Range: 3-24 months (in three-month increments). The default value is 12 months.
Firmware Upgrade Timeout	Specifies the number of minutes to wait, per card, for the GSX firmware upgrade to complete before timing out. Range: 5-30 minutes. The default value is 10 minutes.
LSWU Upgrade Timeout	Specifies the number of minutes to wait for the GSX LSWU to complete before timing out. Range: 60-300 minutes. The default value is 120 minutes.
PIF Write Timeout	Specifies the number of seconds to wait to save the GSX pif file during protection mode check and LSWU initiation. Range: 20-300 seconds. The default value is 60 seconds.
SFTP Client Connect Timeout	Specifies the number of milliseconds to wait for the SFTP client to connect while downloading the GSX installer files from DSI/ NFS while performing a GSX upgrade. The default value is 20000.

Hornet Management Parameters

Parameter	Description
Maximum Connection Wait Time	Specifies the time to wait (in seconds) for a client to connect to Netconf. The default value is 8 seconds.
Maximum Connection Idle Time	Specifies the duration (in seconds) a connection remains idle before terminating. The default value is 960 seconds.
Minimum MINASSH Connection Timeout	Specifies the minimum duration (in seconds) before a MINASSH connection timeout occurs. Range: 20-120 seconds. The default value is 20 seconds. Note In most cases, the default value is sufficient. If the device discovery fails, increase the timeout value in increments until the discovery succeeds.
Minimum MINASSH Connection kex Timeout	Specifies the minimum duration (in seconds) for the key exchange (kex) before a MINASSH connection timeout occurs. Range: 20-120 seconds. The default value is 20 seconds. Note In most cases, the default value is sufficient. If the device discovery fails, increase the timeout value in increments until the discovery succeeds.
Netconf Session Cleaner Thread Running Interval	Specifies the interval (in seconds) for the Netconf session cleaner thread. The default value is 90 seconds.

Hornet Management Ext Parameters

Parameter	Description
Copy SW backup Files if SW backup Base Directory is Changed	Specifies whether to copy software backup files from the old directory to the new directory. • False • True (default)
Software backup Local Directory	Specifies the base directory where all software backups are stored and loaded from RAMP. The default location is <code>/export/home/ems/weblogic/sonusEms/data/\$DEVICETYPE\$/swbackup/</code>
Software backup Remote File	Specifies the file where a software backup is stored and loaded from the device. The default path is <code>/home/admin/saveCdb.tar.</code>
Copy Config Files if Config Base Directory is Changed	Specifies whether to copy config files from the old directory to the new directory. • False • True (default)
Clone Config Base Directory	Specifies the base directory where all exported, edited, and imported configurations are stored. The default path is <code>/export/home/ems/weblogic/sonusEms/data/\$DEVICETYPE\$/</code>
File Download Timeout	Specifies a timeout interval (in seconds) for downloading files from a device. The default value is 900 seconds.
Netconf Session Timeout	Specifies a timeout interval (in seconds) for how long a user can hold an idle session. The default value is 180 seconds.
Max Number of Displayed Instances	Specifies the maximum number of instances to display at a time, for an object. The default value is 100.

List All Parameters

Parameter	Description
Listall Path	Specifies the internal directory path for listall functionality. The default path is <code>/export/home/ems/weblogic/sonusEms/data/cli/internal</code> .
Listall Result Path	Specifies the directory path for listall result files. The default path is <code>/export/home/ems/weblogic/sonusEms/data/cli/listall</code>
Listall Jobs File	Specifies the file to store listall jobs. The default path/filename is <code>/export/home/ems/weblogic/sonusEms/data/cli/listall/CurrentListallJobs</code>
Listall Timeout Minutes	Specifies the number of minutes to elapse for listall jobs to complete before getting terminated by the system. The default value is 60 minutes.
Listall Maximum Jobs Size	Specifies the maximum number of listall jobs to execute at any given time for all the PSXs. The default value is 10.
Listall Maximum Jobs per PSX	Specifies the maximum number of listall jobs to execute at any given time for a given PSX. The default value is 1.
Listall Command File	Specifies the listall command file executed by the system. The default path/filename is <code>/export/home/ems/weblogic/sonusEms/data/cli/internal/listallTable.pl</code>
Listall Perl Path	Specifies the directory path to the perl executable. The default path is <code>/export/home/ems/perl/bin/perl</code>
Listall File Retention Period	Specifies the number of days to retain the Results files. The range is 1-60 days. The default value is 7 days.

LNP Adaptor Parameters

Note

The **LNP Adaptor** option is enabled only when the LNP is deployed.

Parameter	Description
Max Records Count	Maximum number of records to fetch during each synchronization increment. Each IAS can contain different values. Range: 100-10000. The default value is 500.
LNP provisioning batch size	The transaction size of LNP data that are provisioned in batches on PSX. Range: 10-1000. The default value is 100.
Country ID	Specifies the country ID sent to PSX. Range: 1-1000. The default value is 1.
LNP data request timeout	The timeout in seconds for the LNP data request. Range: 1-300. The default value is 30.
Primary PSX Name	The Primary PSX name to use LNP provisioning. This is required when more than one Primary PSX is registered in RAMP. An alarm is generated if the PSX node name is invalid. The Primary PSX name is case sensitive.

MNP Services Parameters

Parameter	Description
Receive Messages From Telcordia MCH	Specifies whether RAMP should start processing broadcast messages from Telcordia MCH. • False – (default) If false, RAMP drops any broadcast message that is sent by MCH. • True – Set to true once bulk data is completely uploaded to all PSXs.

Parameter	Description
Audit Log Update Frequency - Telcordia	Specifies how often (in minutes) to update the audit log with Telcordia statistics. Range: 5-60 minutes. The default value is 5 minutes.
Receive Messages From Syniverse MCH	Specifies whether RAMP should start processing broadcast messages from Syniverse MCH. - False – (default) If false, RAMP drops any broadcast message that is sent by MCH. - True – Set to true once bulk data is completely uploaded to all PSXs.
Audit Log Update Frequency - Syniverse	Specifies how often (in minutes) to update the audit log with Syniverse statistics. Range: 5-60 minutes. The default value is 5 minutes.
Primary PSX Name	The name of the primary PSX to use for mobile number portability (MNP) provisioning. This is required when more than one primary PSX is registered in RAMP. An alarm is generated if the PSX node name is invalid. The name is case sensitive.
Receive Messages From Generic NPC	Specifies whether RAMP should start processing broadcast messages from Generic NPC. - False – (default) If false, RAMP drops any broadcast message that is sent by NPC. - True – Set to True once bulk data is completely uploaded to all PSXs.
Audit Log Update Frequency - Generic NPC	Specifies how often (in minutes) to update the audit log with NPC statistics. Range: 5-60 minutes. The default value is 5 minutes.

NHR Parameters

Parameter	Description
Max Rows to Display	Specifies the maximum number of rows to generate when running on-demand or scheduled reports. The valid range is 1 - 100000. The default value is 500.

Parameter	Description
Reload Report Repository	Specifies whether to reload the report repository to pick up new reports at runtime, without requiring a restart of the RAMP. • False • True This parameter automatically resets to False after a reload.
Discover Network Topology	Specifies whether to run discovery of the entire network topology. This process may take several minutes to complete. • False • True This parameter automatically resets to False after the discovery.
Cancel All Scheduled Reports	Specifies whether to cancel all currently scheduled reports. • False • True This parameter automatically resets to False after the cancellation.
Purger Task Frequency	Specifies how often to run the Purger that removes old records from the database and corresponding archived CSV files. • Every day (default) • Every 2 days • Every week
Purger Task Start Time	Specifies when to start running the Purger task. Subsequent times are determined by Purger Task Frequency. Use the format: (Day of week:hh:mm:AM / PM). For example, Fri:02:30:PM. The default value is Sun:05:00:AM.
Report Retention Period	Specifies the interval of data that the system retains in the database. This setting also affects CSV archive file retention. • None • 1 day • 2 days (default) • 1 week • 2 weeks • 3 weeks • 4 weeks

Node Admin Parameters

Parameter	Description
Node Status Change Purger Task Start Time	Specifies when to run the Node Status Change Purger daily task. Use the format: (hh:mm:[AM/PM]). The default value is 02:00:AM.
Retention period (in days)	Specifies the retention period (in days), entries older than the set duration are removed. The default value is 30 days.
Connection Timeout	Specifies the connection timeout duration (in seconds) for initial socket connection to WRTC. The default value is 30 seconds.
Read Timeout	Specifies the timeout (in seconds) for socket read from WRTC. The default value is 30 seconds.
Max connections	Specifies the maximum number of connections allowed. The range is 10-300 connections. The default value is 50 connections.
Max connections per WRTC	Specifies the maximum number of connections allowed per WRTC. The default value is 5.
Certificate Hostname Verification	Specifies whether to verify the certificate hostname for WRTC. • False (default) • True

PSX CLI Parameters

Parameter	Description
CLI Script Path	Specifies the directory path for PSX CLI scripts. The default path is <code>/export/home/ems/weblogic/sonusEms/data/cli/scripts</code>

Parameter	Description
Script Transaction Size	Specifies the number of commands wrapped in a transaction when executing PSX scripts. The range is 0-11 integers. The default value is 100.
Number of Retries for Deadlocked Transactions	Specifies the number of retries for deadlocked transactions when executing PSX scripts. The range is 0-10 integers. The default value is 3.

RADIUS Parameters

Parameter	Description
GUI Localization	Specifies location used to configure certain fields and forms in the PSX Manager when launched from RAMP using a RADIUS authenticated account. • North America (default) • Generic
Default Country	Specifies the default country for configuring Global User Account information. Select the country from the menu. The default value is 1 - United States of America, Canada and the Caribbean.
Secondary Login Timeout	Specifies the number of seconds a user has to log in using the local login screen after attempting to authenticate through RADIUS, but finding the RADIUS server(s) unavailable. The range is 10-300. The default value is 30 seconds.

Report Framework Parameters

Parameter	Description
CSV Reports Archive Base Directory	Specifies the base directory for writing CSV reports. The default directory is <code>/opt/sonus/ems/weblogic/sonusEms/data/report_archive</code>
Max Scheduled Threads	Defines the maximum number of threads to use for scheduled report execution. The range is 1-4. The default value is 2.

Note

You must restart RAMP for this new thread setting to take effect.

SBC GUI Parameters

Parameter	Description
Enable SSO	Specifies whether to enable SSO. • False – The SBC Configuration Manager login page launches before accessing the SBC Configuration Manager. • True – The SBC Configuration Manager is accessed directly from RAMP and is no login required.

SGX API Parameters

Parameter	Description
Deploy version 5.2.1	Specifies whether to deploy SGX API 5.2.1. • False • True (default)

SBC API Parameters

Parameter	Description
Connection Timeout	Specifies the timeout (in seconds) for initial socket connection to the SBC Core. The range is 10-120 seconds. The default value is 30 seconds.
Read Timeout	Specifies the timeout (in seconds) for socket read from the SBC Core. The range is 10-5400 seconds. The default value is 30 seconds.
Max connections	Specifies the maximum number of outbound connections allowed from RAMP to the SBC Cores. The range is 10-300. The default value is 50.
Max connections per SBC Core	Specifies the maximum number of connections allowed per SBC Core. The range is 1-10. The default value is 2.

Parameter	Description
Protocol	Specifies the protocol to use to connect the SBC Core. • https (default) • http
Connection Port	Specifies the connection port to use to connect to the SBC Core. 0-11 integers. The default value is 443.
SBC Core Datastore	Specifies the SBC Core datastore to use to access configuration entities. The default value is <code>config</code> . Note Ribbon recommends you contact Product Support before modifying the default value.
SBC Core status Datastore	Specifies the SBC Core datastore to use to access status entities. The default value is <code>operational</code> . Note Ribbon recommends you contact Product Support before modifying the default value.
Certificate Hostname Verification	Specifies whether to perform certificate hostname verification. • False (default) • True

SBC Management Parameters

Parameter	Description
Successful Audit Purger Frequency (in days)	Specifies how long to retain successful audit purger details. • 1 day (default) • 2 days

Parameter	Description
Failed Audit Purger Frequency (in days)	Specifies how long to retain failed audit purger details. The range is 7-14 days. The default value is 7 days.
Completed Job Purger Frequency (in days)	Specifies how long to retain completed job purger details. The range is 0-7 days. The default value is 7 days.
Job Purger Task Start Time	Specifies when to run the job purger daily task. Use the format: (hh:mm:[AM/PM]). Example: 02:30:AM.
Audit Purger Task Start Time	Specifies when to run the audit purger daily task. Use the format: (hh:mm:[AM/PM]). Example: 02:30:AM.
Backup Catalogue Purger Task Start Time	Specifies when to run the backup catalogue purger daily task. Use the format: (hh:mm:[AM/PM]). Example: 02:30:AM.
Connection Timeout (in seconds)	Specifies the SFTP connection timeout. 0 specifies an infinite timeout. The range is 0-3600 seconds. The default value is 213 seconds.
Upgrade Status Check Retry Interval (in minutes)	Specifies the upgrade status-check retry interval, after the upgrade starts. This is used for SBC Core upgrade. The range is 5-20 minutes. The default value is 10 minutes.
Upgrade Status Check Retry Interval for SBC Edge (in minutes)	Specifies the upgrade status-check retry interval, after the upgrade starts. This is used for SBC Edge upgrade. The range is 3-10 minutes. The default value is 3 minutes.
Upgrade Status Check Retry Count	Specifies the upgrade status-check retry count, after the upgrade starts. The upgrade is considered failed if the retry count is exhausted. This is used for all upgrade types. The range is 6-144. The default value is 18.

Parameter	Description
Upgrade Status Check Retry Count Increment per Upgrade Order	Specifies the upgrade status-check retry count increment per order in the waiting queue. This is used for SBC Core upgrade. The range is 1-240 seconds. The default value is 10 seconds.
Upgrade Status Check Retry Count Increment per Upgrade Order for SBC Edge	Specifies the upgrade status-check retry count increment per order in the waiting queue. This is used for SBC Edge upgrade. The range is 1-240 seconds. The default value is 15 seconds.

Telnet Session Manager Parameters

Parameter	Description
Telnet Connect Timeout	Specifies the timeout value for connecting to Telnet through GSX, SBC Core and SGX. • 1 second • 2 seconds • 4 seconds (default) • 8 seconds • 16 seconds
Telnet Retry Time	Specifies the timeout value for retrying to connect to Telnet through GSX, SBC Core and SGX. • 2 seconds • 4 seconds • 6 seconds • 8 seconds • 10 seconds (default) • 20 seconds • 30 seconds • 1 minute • 2 minutes • 5 minutes • 10 minutes • 15 minutes • 30 minutes

Parameter	Description
Telnet Read Timeout	Specifies the timeout value for reading GSX, SBC Core and SGX Telnet response. • 16 seconds • 32 seconds • 64 seconds • 128 seconds (default) • 192 seconds • 256 seconds • 320 seconds • 640 seconds • 1280 seconds
Telnet Wait Timeout	Specifies the timeout value for waiting for GSX, SBC Core and SGX telnet response. This value specifies how long RAMP waits for the release of a Telnet connection by other users before sending a timeout message to a waiting user. If necessary, increase the Wait Timeout to allow for high network traffic. Setting this value too high potentially increases the response time. • 1 second • 2 seconds • 4 seconds • 8 seconds • 16 seconds • 32 seconds (default) • 64 seconds • 128 seconds • 192 seconds
Telnet Idle Timeout	Specifies the timeout value for an idle GSX, SBC Core and SGX telnet session. The Idle Timeout ensures that the RAMP does not consume the limited number of Telnet sessions a GSX supports. The RAMP maintains a session (even when not in use) in anticipation of follow-up requests to the connected GSX. This reduces any connecting/disconnecting overhead. If a connection remains inactive for the specified period, the session disconnects. • 2 minutes • 5 minutes (default) • 10 minutes • 15 minutes • 20 minutes • 25 minutes • 30 minutes

Parameter	Description
Maximum Telnet sessions per GSX	Specifies the maximum number of Telnet sessions allowed per GSX (i.e., the maximum number of concurrent Telnet connections that the RAMP can open for each GSX). The GSX supports a maximum of eight simultaneous connections; however, you may want to reserve sessions so users can Telnet directly to a GSX. The range is 1-8 sessions. The default value is 4 sessions.
Maximum Telnet Sessions per SBC Core	Specifies the maximum number of Telnet sessions allowed per SBC Core (i.e., the maximum number of concurrent Telnet connections that the RAMP can open for each SBC). The SBC supports a maximum of eight simultaneous connections; however, you may want to reserve sessions so users can Telnet directly to an SBC. The range is 1-6 sessions. The default value is 4 sessions.
Maximum Telnet Sessions per SGX	Specifies the maximum number of Telnet sessions allowed per SGX. The range is 1-6 sessions. The default value is 4 sessions.
Allow CLI session to non-SSO SBX	This option allows CLI sessions to older SBC versions that do not support SSO. • True: (default) The RAMP CLI session is established for SBCs with older versions prior to 11.x. • False: The RAMP CLI session is not established for SBCs with older versions prior to 11.x.

Trunkgroup Validator Parameters

Parameter	Description
Trunk Group validation	Specifies whether to enable trunk group existence validation. • False (default) • True

UI Gen Parameters

Parameter	Description
Check Models Update	Specifies whether to enable model file changes. • False (default) • True

Parameter	Description
Model Scanning Interval	Specifies model files scanning interval (in milliseconds). The range is 0-600000000 milliseconds. The default value is 60000 milliseconds.

Utilities Parameters

Parameter	Description
Minimum thread-pool size	Specifies the minimum number of threads in the RAMP thread pool. 0-1234567890 threads. The default value is 10 threads.
Maximum thread-pool size	Specifies the maximum number of threads in the RAMP thread pool. 0-1234567890 threads. The default value is 40 threads.
CDR Search timeout value	Specifies the timeout value (in milliseconds) for the Call History Report generation tool to avoid a time-out during the parsing of large ACT files. The range is 10000-300000 milliseconds. The default value is 10000 milliseconds.
Timeout for FTP Connections	Specifies the timeout value (in seconds) for FTP connections to test the FTP credentials during device discovery. Range: 1-25. The default is 2 seconds.
PSX Manager restricted to 10.3 or later	Specifies whether to restrict PSX Manager to version 10.3 or later. - False – (default) Access is allowed to all versions. - True – Access is only allowed to PSX 10.3 or later versions.
Status of Ctrl+Alt+Del configuration	Specifies whether to enable the Ctrl+Alt+Del feature. - False (default) - True The default is False.

Parameter	Description
Ctrl+Alt+Del configuration - Count	Note This parameter is not supported. Specifies the number of times to receive the Ctrl+Alt+Del signal within the period specified by Time Period. Range: 3-6. The default is 5.
Ctrl+Alt+Del configuration - Time Period	Note This parameter is not supported. Specifies the time period (in seconds) to receive the number of Ctrl+Alt+Del signals specified by Count. Range: 1-6. The default is 1 second.
REST Client Establish Connection Timeout	Specifies the timeout duration (in seconds) when trying to make initial socket connection. If you change this value, you must restart the RAMP for the updated value to take effect. Range: 5-120 seconds. The default is 30 seconds.
REST Client Socket Timeout	Specifies the timeout duration (in seconds) for socket inactivity. If you change this value, you must restart the RAMP for the updated value to take effect. Range: 5-120 seconds. The default is 30 seconds.
REST Client Connection Pool Size	Specifies the number of connections that are allowed to be pooled. If you change this value, you must restart the RAMP for the updated value to take effect. Range: 10-1000. The default is 500.
REST Client Connection Pool Size per Route	Specifies the number of connections to pool per URL. If you change this value, you must restart the RAMP for the updated value to take effect. Range: 1-3. The default is 2.
PM Micro Service IP Address	IP Address of the PM microservice. Supports IPv4 and IPv6 addresses.

Parameter	Description
Certificate Hostname Verification	Specifies whether to perform certificate hostname verification for the PM microservice. • False (default) • True
PM Micro Service REST Client Connection Establishment Timeout	Specifies the timeout duration (in seconds) to make an initial socket connection to the PM microservice. If you change this value, you must restart the RAMP for the updated value to take effect. The range is 5-120 seconds. The default is 30 seconds.
PM Micro Service REST Client Socket Timeout	Specifies the timeout duration (in seconds) for socket inactivity. If you change this value, you must restart the RAMP for the updated value to take effect. The range is 5-120 seconds. The default is 30 seconds.
PM Micro Service REST Client Connection Pool Size	Specifies the number of connections allowed to pool. If you change this value, you must restart the RAMP for the updated value to take effect. The range is 10-1000 connections. The default is 500 connections.
PM Micro Service REST Client Connection Pool Size per Route	Specifies the number of connections to pool per URL. If you change this value, you must restart the RAMP for the updated value to take effect. The range is 1-3 connections. The default is 2 connections.
Filesystem Cleanup Percentage	Specifies the percentage of filesystem usage which triggers cleanup of the <code>/opt</code> partition. The range is 0-100. The default is 60.
Maximum CDR file age (in days)	Specifies the maximum number of days to keep CDRs in the <code>/opt</code> partition. The range is 1-365. The default is 7.
Enable CLI/API username logging	Specifies whether to enable logging of RAMP CLI/API user name for CLI/API operations. Navigate to PSX Manager GUI > admin > audit log to view the logs. • False (default) • True

Change IP Address

Use this procedure to change the management IP address of Ribbon Application Management Platform (RAMP) to be able to connect to a different RAMP.

Prerequisites

RAMP should be up and running.

Start

1. Log on to the KVM/VMWare host and access the RAMP console.
2. As Insight user stop RAMP and `emsMgmt` processes:

```
#/opt/sonus/ems/emsMgmt stop
```

3. Login as root user to disable and stop the `opensaf` processes:

```
#sudo su
#systemctl disable opensafd.service
#systemctl stop opensafd.service
```

4. Access the file where the IP addresses are stored:

```
vi /etc/hosts
```

5. To edit and change the IP address::
 - a. Using `nmtui` you can edit the connection, deactivate, and then activate. Run the `nmtui` and perform the following:
 - i. To change the existing IP address, for example, if the new RAMP IP is 192.168.199.47, then:

```
eth0> 192.168.199.47
```

- ii. Deactivate the new connection in the `nmtui`:

```
nmcli con down eth0
nmcli con up eth0
```

- iii. Restart the network manager service:

```
systemctl restart NetworkManager.service
```

- b. To view if the IP address is changed, run the following command. You will see the new IP address.

```
ifconfig
```

6. At the prompt, change to `root` user:

```
sudo su
```

7. Navigate to the configuration directory and change the RAMP IP address (for example if the new IP is 192.168.199.47):

```
cd /opt/sonus/ems/conf/  
./changeIpAddress.sh -i 192.168.199.47 -d -l /tmp/ChangeIPAddress.log
```

8. Using the new IP address, log on to RAMP as admin user.
9. Switch to root user:

```
sudo su
```

10. Start and enable `opensaf` :

```
systemctl start opensafd.service  
systemctl enable opensafd.service
```

When `Opensaf` is enable and active, it starts RAMP.

11. You can check the `opensaf` status in the log file by accessing the `emsProcMgmt.log` file. Navigate to the log file:

```
/opt/sonus/ems/logs/emsProcMgmt.log
```

12. To check if all the processes are running, run the following commands to change to `insight` user and check the status:

```
su - insight  
/opt/sonus/ems/emsMgmt status
```

13. You can now disassociate and associate all the registered nodes with the old IP address. Refer to [Modify Managed Device Association](#).

System Activity Logging

In this section:

- [View the System Activity Log](#)
- [View Live System Activity Messages](#)

Ribbon Application Management Platform (RAMP) provides a system activity log (`ems_trace_log`) that records system activities and error conditions. Because of the large number of records in the system log, RAMP provides controls to filter and search the list. It also provides an option to view log activity as it occurs.

Use the following procedures to open and work with the system activity log.

View the System Activity Log

To view recent system activity log entries:

1. Log on to the RAMP GUI.
2. Navigate to **System > Troubleshooting > System Activity**.
3. In **Num Lines**, enter the number of records you want to display. The minimum is 5000.
4. Click **View Log**. The log entries appear with the oldest entries first.

To Search Within the System Activity Log

On the **System Activity** window:

In **Filter**, enter a search value and then click **Search**.

To Filter Out Warning Messages

You have the option to disable logging of warning messages in the system activity log. This filtering applies to records added to the log file going forward.

On the **System Activity** window:

1. Click **Log Filter** to open the **System Activity Log Filter** window.
2. Click to uncheck the **Enable Logging: Warning** check box.
3. Click **Apply**.

View Live System Activity Messages

The listing of log entries in the main **System Activity** window does not refresh automatically. However you can open a window to monitor system activity messages as they occur.

On the **System Activity** window:

Click **Live Log** to open the **Live System Activity** window.

Live System Activity Controls

In the **Live System Activity** window you can:

- Click **Pause** to temporarily pause the display of new log entries.
- Click **Copy** to copy the current contents of the window to the clipboard so that you can paste it in another location.
- Click **Clear** to clear the current contents of the window and continue displaying new entries.
- Enter a filter value in the **Filter by** field to display only entries containing the search term.

Exporting Logs to a Remote Syslog Server

In this section:

- [Overview](#)
- [Sample Configuration file \(/etc/rsyslog.conf\) for Remote Syslog Server](#)

Overview

Ribbon Application Management Platform (RAMP) supports sending application and system level logs to a Remote Syslog server, including user activity logs. To enable sending logs to an external location you must provide the remote Syslog Server IP address in the RAMP GUI by navigating to **System > Interfaces > Logs**. To receive the logs on the Remote Syslog server, edit the configuration in the file `/etc/rsyslog.conf` which determines the facility through which the logs are received.

Note

Upon upgrade of RAMP, you must apply the configuration on the RAMP GUI by navigating to **system > interface > logs** to enable log forwarding.

Note

The default transport protocol used is TCP. If you want to change it to UDP, the you must include the parameter `SYSLOG_TRANSPORT` in the `SystemConfig.txt` file by navigating to `/opt/rbbn/ems/weblogic/sonusEms/data/sys/SystemConfig.txt`.

For example,

`SYSLOG_TRANSPORT=UDP`

The parameter `SYSLOG_TRANSPORT` is not present initially in `SystemConfig.txt`. Add this parameter only if you change the transport protocol.

Use the following procedure to provide the remote Syslog server address:

Start

1. Log on to the RAMP GUI.
2. Navigate to **System > Interfaces > Logs**.
3. In **Remote Syslog server IP**, enter the IP address of the remote Syslog server. If you want to enter multiple IP addresses, separate them with a comma (,). You can also specify a different port number other than the default port (514). For example (17.52.19.229:528,17.52.19.239:514).

Note

Please enter a valid IP address. Invalid IP address may lead to failure.

4. Click the adjacent checkbox to enable sending logs to the remote server.
5. **Enable/Disable** the **State** of services using the radio button to forward the logs to remote syslog servers.
6. Modify the **Facility** for each microservice based on the following table:

Note

Enter a valid facility. If there is an invalid facility, RAMP uses the default syslog facility (local6). Do not modify the facility for system logs.

Service	Facility
System	Set to "default". The default value contains logs from: ◦ authpriv ◦ cron ◦ ftp ◦ local1 ◦ local2 ◦ local7 ◦ mail ◦ user This value is not changeable.
PM	local0
FM	local1
DM	local2
LM	local3
AA	local4
EMA	local5
httpd	local6
kafka	local6
Insight	local6
DBaaS	local6
Opensaf	local6

7. Click **Apply**.

Sample Configuration file (/etc/rsyslog.conf) for Remote Syslog Server

Here is a sample configuration file `/etc/rsyslog.conf` for the Remote Syslog Server. Please modify this based on your requirements.

```

# rsyslog configuration file

# For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html
# or latest version online at http://www.rsyslog.com/doc/rsyslog_conf.html
# If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html

#### MODULES ####

module(load="imuxsock"      # provides support for local system logging (e.g. via logger
command)
        SysSock.Use="off") # Turn off message reception via local log socket;
        # local messages are retrieved through imjournal now.
module(load="imjournal"     # provides access to the systemd journal
        StateFile="imjournal.state") # File to store the position in the journal
#module(load="imklog") # reads kernel messages (the same are read from journald)
#module(load="immark") # provides --MARK-- message capability

# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
#module(load="imudp") # needs to be done just once
#input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")

#### GLOBAL DIRECTIVES ####

# Where to place auxiliary files
global(workDirectory="/var/lib/rsyslog")

# Use default timestamp format
module(load="builtin:omfile" Template="RSYSLOG_TraditionalFileFormat")
module(load="imfile" mode="inotify")

module(load="mmutf8fix") #if $fromhost-ip == "10.0.0.1" then
action(type="mmutf8fix")

# Include all config files in /etc/rsyslog.d/
include(file="/etc/rsyslog.d/*.conf" mode="optional")

$template myFormat,"%msg%\n"
$ActionFileDefaultTemplate myFormat

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                          /dev/console

# Log anything (except mail) of level info or higher.

```

```

# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none;local0.none;local1.none;local7.none -/var/log/
ramp_system.log
Note: Add local7.none along with location of log file to redirect default logs to
specified log file.

if $syslogtag contains 'lsyncd:' then /var/log/lsyncd/lsyncd.log
else /var/log/messages # This will contain application and system logs which can be
stored in a custom file instead of messages

# The authpriv file has restricted access.
authpriv.* /var/log/secure

# Log all the mail messages in one place.
mail.* -/var/log/maillog

# Log cron stuff
cron.* /var/log/cron

# Everybody gets emergency messages
*.emerg :omusrmsg:*

# Save news errors of level crit and higher in a special file.
uucp,news.crit /var/log/spooler

# Save boot messages also to boot.log
local7.* /var/log/boot.log

#local0.info /var/log/ems/opensaf_audits.log

local1.info /var/log/ems/ems_login.log

#local0.debug /var/log/ems/opensaf_components_health.log

local0.* /var/log/pm.log
local1.* /var/log/fm.log
local2.* /var/log/dm.log
local3.* /var/log/lm.log
local4.* /var/log/aa.log
local5.* /var/log/ema.log
local6.* /var/log/insight.log

```

```
# Severity levels can also be linked to facility

local0.info                /var/log/PMTestI.log
local0.debug               /var/log/PMTestD.log
local1.info                /var/log/FMTestI.log
local1.debug               /var/log/FMTestD.log
local2.info                /var/log/DMTestI.log
local2.debug               /var/log/DMTestD.log
local3.info                /var/log/LMTestI.log
local3.debug               /var/log/LMTestD.log
local4.info                /var/log/AATestI.log
local4.debug               /var/log/AATestD.log
local5.info                /var/log/EMATestI.log
local5.debug               /var/log/EMATestD.log
local6.info                /var/log/HTTPDTestI.log
local6.debug               /var/log/HTTPDTestD.log
local7.info                /var/log/ramp_systemI.log
local7.debug               /var/log/ramp_systemD.log

# ### sample forwarding rule ###
#action(type="omfwd"
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#queue.filename="fwdRule1"      # unique name prefix for spool files
#queue.maxdiskspace="1g"       # 1gb space limit (use as much as possible)
#queue.saveonshutdown="on"     # save messages to disk on shutdown
#queue.type="LinkedList"       # run asynchronously
#action.resumeRetryCount="-1"   # infinite retries if host is down
# Remote Logging (we use TCP for reliable delivery)
# remote_host is: name/ip, e.g. 192.168.0.1, port optional e.g. 10514
#Target="remote_host" Port="XXX" Protocol="tcp")
$FileCreateMode 0640
local3.* /var/log/sftp.log
input(type="imfile"
    File="/opt/sonus/auth/logs/userActivity.log"
    Tag="user-activity"
    Severity="info"
    Facility="local2")
```

Device REST Credentials

Cloud-based devices that dynamically register with Ribbon Application Management Platform (RAMP) must provide a REST user ID and password during the registration process. For registration to be successful, those responsible for instantiating cloud-based nodes must be aware of the valid REST credentials. The parameters on the **Device REST Credentials** window specify what these parameters are for your RAMP system.

Use the following procedure to configure REST credentials for your system.

Start

1. Log onto the RAMP GUI.
2. Navigate to **System > Interfaces > Device REST Credentials**
3. In **REST Username**, enter a name for the REST user. The default username is "restuser," with a default password of "sonus123."

4. In both **REST Password** and **Re-Enter Password**, enter the new password.
5. Click **Apply**.

Note

If you change the REST credentials, update any instantiated cloud nodes with the new credentials.

SSH Active Channels

The Ribbon Application Management Platform (RAMP) uses Secure Shell (SSH) to connect with registered PSX devices. The table on the **SSH Active Channels** window provides details on RAMP's current SSH connections to PSX devices. Under some circumstances, you may be instructed by Ribbon Product Support to terminate a connection. This might be to clear stale connections or as a troubleshooting step.

Use the following procedure to view and optionally terminate an active SSH channel.

Start

1. Log onto the RAMP GUI.
2. Navigate to **System>Interfaces>SSH Admin>Active Channels**. The list of active SSH channels appears.
3. To terminate a channel, click the **Terminate** action button in the row of the channel you want to terminate.

RAMP Profile Settings

Use the **RAMP Profile Settings** window to determine which features are accessible in the Ribbon Application Management Platform (RAMP) graphical user interface (GUI) and which device types appear in the Node Registration window. The changes you make to **RAMP Profile Settings** apply to the system as a whole and therefore change the view for all users.

Some components of the RAMP GUI cannot be disabled, but the profile settings give you the option to remove menu items and windows for some features if they do not apply to your specific deployment. Note that the list of features that you cannot disable is summarized on the window.

Use the following procedure to configure RAMP profile settings for your system.

Prerequisites

You have Super User [privileges](#) for **Insight Administration** within the **Core Resources** application.

Start

1. Log onto the RAMP GUI.
2. Navigate to **System > Settings > RAMP Profile Settings**
3. In the **Global Feature Availability** area, use the toggle controls to enable or disable services and features in the RAMP GUI. By default all options are enabled.

Feature	Description
Fault Management	Controls whether the Fault Management options appear under Observability.
Performance Management	Controls whether the Performance Management options appear under Obser

Feature	Description
Backup	Controls whether the Backup options appear under Operations. Note that Backup options do not appear in the GUI until at least one device of those types is registered.
Health Reports	Controls whether the Health Reports options appear under Operations.
Provisioning	Controls whether the Provisioning options appear under Operations. Note that the Provisioning options do not appear in the GUI until at least one device of those types is registered.
Upgrade	Controls whether the Upgrade options appear under Operations. Note that the Upgrade options do not appear in the GUI until at least one device of those types is registered.

4. In the **Global Node Type Registration** area, use the toggle controls to select which types of devices appear in the Device list when registering devices or creating clusters. By default all device types are enabled.
5. Click **Save Settings** to apply your changes.

Database Configuration

Use the **Database Configuration** window to modify Ribbon Application Management Platform (RAMP) database connection settings if you are directed to do so by Ribbon Product Support. Otherwise, to ensure proper database operations, these settings should not be changed.

Use the following procedure to access the **Database Configuration** window when directed.

Start

1. Log onto the RAMP GUI.
2. Navigate to **System > Settings > Database Configuration**
3. Enter a new value in **Maximum Connections**, if directed. This setting specifies the size of the database connection pool RAMP uses to communicate with the database. An insufficient value can cause data to be dropped and application errors. The minimum value is 6 and maximum is 100. Ribbon recommends a value of 40, which is the default.
4. Enter a new value in **Connection Timeout**, if directed. This setting specifies how long RAMP will wait for a connection to the database before timing out. The default is 30 seconds. RAMP logs an error in the system log for each timeout that occurs.
5. Restart RAMP to apply the change.

PSX Call Trace Destination

Use the **Trace Destinations** window to provision or change where PSX call traces are sent. By default, the traces are directed to the Ribbon Application Management Platform (RAMP) deployment with which the PSX is registered. On the RAMP that manages the PSX, this default destination is indicated by the value `localhost:9004`. Configure the trace destination option on primary PSX Policy Servers. The primary PSX propagates the trace destination information to each of its replica PSXs.

Use the following procedure to configure the trace destination for a PSX.

Prerequisites

You have Super User [privileges](#) for the **Insight Administration** resource within the **Core Resources** application.

Start

1. Log onto the RAMP GUI.
2. Navigate to **System > Settings > PSX Policy Server > Trace Destinations**. A list of registered primary PSX devices appears.
3. In the **PSX Policy Server** list, locate the primary PSX whose trace destination you want to change and enter the new destination in the corresponding **Trace Destination** field. Enter either the hostname or the IP address, followed by a colon and the port number. For example, `10.10.10.10:9004`.
4. Click **Update**. This change does not require a reboot of the PSXs.

PSX Manager Version Compatibility

Use the **PSX Manager Version** window to review the list of PSX Manager versions that are supported by the currently installed version of the [Ribbon Application Management Platform \(RAMP\) application](#). If the version of the PSX you want to run is not listed, you must install the comparable version of PSX Manager.

Use the following procedure to access the **PSX Manager Version** window to review the list of PSX Manager versions to determine if a different version is required.

Start

1. Log onto the RAMP GUI.
2. Navigate to **System > Settings > PSX Policy Server > PSX Manager Versions**
3. If you load a new version of PSX Manager, click **Reload** to make it available. It is not necessary to restart RAMP.

GSX User Interface

In this section:

- [Restrict Access to GSX Commands](#)
- [Configuration Files for GSX Navigator and Task Configurator](#)
- [Set GSX Navigator Discovery](#)
- [Sort GSX Trunk Groups](#)

Use the windows under **GSX User Interface** to configure options related to using the user interface that you launch from Ribbon Application Management Platform (RAMP) to configure GSX devices.

Restrict Access to GSX Commands

The Ribbon Application Management Platform (RAMP) users with Administrative privileges can restrict the access to GSX Navigator commands based on the roles.

For example, if the administrator places a restriction on the “TRUNKGROUP:Delete” command with respect to the role “default”, then users associated with the “default” role are unable to view (or execute) the “TRUNKGROUP:Delete” command.

Start

1. Log onto the RAMP GUI.
2. Navigate to **System > Settings > GSX User Interface > Command Access Control**. The GSX commands display.
3. Locate the command you want to restrict. The same command may be bound to more than one object. With the cursor in the list, use **<CTRL>F** to open a search dialog box.
4. Enter the **Role** at the end of the line. Separate multiple entries with commas. When typing the role, ensure that it is typed exactly as it appears (case sensitive). A list of valid roles appears above the

command list. To ensure accuracy, copy a role name from this location and paste it in the appropriate location(s).

5. Click **Apply**. You are prompted to confirm.
6. Click **OK** to confirm the changes.

Configuration Files for GSX Navigator and Task Configurator

Use the Configuration Files page to open a user interface that allows you to designate and/or reload new Command Configuration and Task Configuration files. Only Ribbon technicians should initiate changes to these files. Any changes to these files directly affect the proper operation of the GSX Navigator and Task Configurator.

Note

Close all open Task Lists within the Task Configurator before reloading Command and Task Based Configurations.

Start

1. Log onto the RAMP GUI.
2. Navigate to **System > Settings > GSX User Interface > Configuration Files**. The **Configuration Files** window opens.
3. Use the following table to configure the parameters and then click **Save**.

Configuration File Settings

Setting	Description
Command and Task Based Configuration File	This configuration file contains commands executed from the GSX Navigator and Tcl Procs executed from the Task Configurator.
Reload Command and Task Configurations	Reloads the GSX Navigator and Task Configurator software with changes to their respective configuration files.
Refresh Trunk Group Validator Cache	Refreshes the PSX Trunk Group on Ribbon Application Management Platform (RAMP).
Enable Core GSX entity Authorization	Enables core GSX entity access restriction after upgrading from Release 8.3 or later. By default, the core GSX entity access restriction is enabled after installation. To modify GSX Management privilege levels, see Set Privileges for Users by Adding Roles.

Setting	Description
Note To automatically enable core GSX entity authorization after upgrade, set <code>EnableCoreGSXentityAccess</code> to true in the SystemConfig.txt file. The SystemConfig.txt file is available in the following location: <code><BASE_DIR>/weblogic/sonusEms/data/sys/SystemConfig.txt</code>	

Set GSX Navigator Discovery

Ribbon Application Management Platform (RAMP) users with administrative privileges can select tree discovery type for the GSX Navigator tree. RAMP does not do full discovery when the GSX navigation tree is not in use. The system updates the navigation tree for a given GSX only when displaying the tree.

Start

1. Log onto the RAMP GUI.
2. Navigate to **System > Settings > GSX User Interface > Discovery Parameters**. The **GSX Discovery Type Configuration** pane displays.
3. Select one of the following options:
 - **manually**: Click the Discover new tree button to initiate a discovery manually, updating the tree with the latest data.
 - **automatically**: When tRAMP receives the PIF trap that indicates the GSX configuration has changed, the system initiates a full discovery, automatically updating the tree with the latest data.
 - **optimally** (default): When RAMP receives the PIF trap that indicates the GSX configuration has changed, a full discovery is initiated, updating the tree with the latest data only if it is not aware of the configuration changes.
4. Click **Apply**. The discovery type for GSX Navigator is updated.

Sort GSX Trunk Groups

Ribbon Application Management Platform (RAMP) allows you to select the ordering algorithm for displaying GSX trunk group in GSX Navigator. You can select to display the trunk group names in either alphanumeric or alphabetical order.

Start

1. Log onto the RAMP GUI.
2. Navigate to **System > Settings > GSX User Interface > Trunk Group Ordering**. The **Insight Trunk Group Ordering** pane displays.
3. Select one of the following options:
 - **Alphanumerically**: The alphabetical prefix of the trunk group names are ordered alphabetically and the numeric suffix of the trunk group names are sorted in ascending order.
For example, tg10, tg25, tg40, tg50, tg100, tg300 tg5abc, tg5abc1, tgabc2, tg5abc110, tga, tgb
 - **Alphabetically**: The trunk group names, in their entirety, are sorted alphabetically. For example, tg10, tg100, tg25, tg300, tg40, tg50, tg5abc, tg5abc1, tg5abc110, tg5abc2, tga, tgb
4. Click **Apply**. The sorting order for displaying GSX trunk groups is set.

SSH Configuration

In this section:

- [Configure SSH Properties](#)

You must enable the use of SSH by setting the path to the SCP executable and the SSH installation path. You can perform this task by editing the `ssh.properties` file manually (`scpCmd` and `sshPath` parameters). You must stop and restart the RAMP for the changes to take effect.

Before enabling or disabling the SSH Configuration, terminate all the connections from RAMP to PSX. These connections include PSX Manager, CLI, API, and LNP tools.

After updating and discovering the PSX with the new SSH configuration, restart the services that connect to the PSX.

Configure SSH Properties

To configure SSH properties:

1. Log on to the RAMP CLI as the admin user.
2. Change to the Insight user:

```
sudo su - insight
```

3. Edit the following file:

```
/opt/sonus/ems/weblogic/insight/ems/resources/properties/main/properties/ssh.properties
```

4. Enter or modify the values. The following table represents the parameters in `ssh.properties`:

Parameter	Description	Mandatory (M)/ Optional (O)	Range with example
idleTunnelGraceMillis	The interval in milliseconds to terminate idle SSH tunnels. The idle tunnels are discarded after the set interval.	M	1 - 120
defaultSshEnabled	The flag to enable SSH.	M	◦ FALSE ◦ TRUE (default)
sshPort	The PSX port used for SSH.	M	22 (default)

Parameter	Description	Mandatory (M)/ Optional (O)	Range with example
sshPath	The SSH installation directory.	M	/usr (default)
scpCmd	The path to SCP executable.	M	/usr/bin/scp (default)
sshTunnelConnect Attempts	The count of attempts for connecting to the SSH tunnel.	M	5 (default)
sshTunnelCreation Delay	The interval in milliseconds for the RAMP to wait until an SSH tunnel is created.	M	400 (default)
directSshNotSupportedTypes	The device types not supported for direct SSH connection on the RAMP.	M	
sshReadTimeoutSecs	The interval in seconds to wait for the SSH response.	M	60 (default)
scpTransferTimeout Secs	The interval in seconds to wait for the SCP response.	M	300 (default)
minaSshProps	Apache MINA SSH timeout interval properties.	M	idle-timeout 18000000 long,nio2-read-timeout 18030000 long,heartbeat-interval 60000 long
minaIoThreads	The count of IO threads used by the MINA SSH library.	O	10 - 15 default: 10
sshChannelOpenWaitTimeout	The timeout interval for the thread to wait until the channel gets opened. If the channel does not open before timeout, it shows "SSH Exception".	O	15000 - 60000 default: 60000

5. Save the file.
6. Restart the RAMP for the changes to take effect.

RAMP Tools

In this section:

- [Call Trace](#)
- [Call History](#)
 - [Call History Settings](#)
- [Inventory](#)
- [Report Scheduler](#)
- [Trunk Group](#)
 - [Renaming Trunk Groups](#)
- [GSX System](#)
- [Number Portability Services](#)
 - [Mobile Number Portability](#)
 - [Local Number Portability](#)

Ribbon Application Management Platform (RAMP) provides tools you can use to visualize data from managed SBC Core devices.

- [Call Trace](#) – to view call traces initiated on a selected SBC device.
- [Call History](#) – to generate call history reports derived from Call Detail Records (CDRs) from a selected SBC device.
- [NP Services](#) – for configuring number portability services.

The articles in this section describe these tools.

Call Trace

Related articles:

- [Call Trace and Packet Capture - Call Trace \(SBC Core\)](#)
- [Call Trace \(GSX\)](#)
- [PSX Call Trace Destination](#)

Ribbon Application Management Platform (RAMP) provides an interface to view call traces initiated on managed SBC Core/GSX devices. Call trace information can be used in debugging policy and call routing issues. The options for configuring call trace filters and for initiating call traces are set on the SBC device, however the traces themselves can be viewed on RAMP.

- Refer to [Call Trace and Packet Capture - Call Trace](#) for information on call trace configuration on the SBC.
- Refer to [Call Trace](#) for information on call trace configuration on the GSX.
- Refer to [PSX Call Trace Destination](#) for information on call trace configuration on the PSX.

Use the following procedure to select call trace information from the SBC Core device/GSX or from logs stored on an associated PSX.

Note

Use of Call Tracing can have significant impact on the network performance of an SBC/GSX and its associated PSX Policy Server. Ribbon strongly recommends that you take great care in configuring call trace filters, that result in only a small number of calls being traced. Ribbon also recommends that you delete a call trace filter once you have obtained the necessary information.

Prerequisites

- Call Trace Filter configuration is completed on the SBC Core/GSX device and call traces have been run.
- You have Super User [privileges](#) for **Tools** within the **Core Resources** application.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Tools > Call Trace**
3. To retrieve call trace information for a specific SBC Core device:
 - a. In **Node Type**, select **SBC Core / GSX**.
 - b. In **Node List**, select an SBC Core/GSX device.
 - c. In **Filter**, select a call trace filter to define which call trace logs to view. The list contains the names of call trace filters configured on the selected SBC/GSX device.
 - d. In **Records**, enter the number of records you want to view between 1 and 2048 (default).
 - e. In **Sort by**, select an option for sorting the records: **GCID** (global call identifier), **ICID** (IMS charging identifier), or **Time**.
 - f. Click **View**. RAMP applies the selected filter for the selected SBC Core/GSX device and displays the matching call trace information.
4. To retrieve call trace information for a specific PSX device:
 - a. In **Node Type**, select **PSX**.
 - b. In **Node List**, select a PSX device.
 - c. Click **View**. RAMP displays the unfiltered call trace information for the selected PSX.

Call History

Related articles:

- [Call History Settings](#)

Ribbon Application Management Platform (RAMP) provides an option to generate call history reports derived from Call Detail Records (CDRs) from a selected SBC Core device. When generating these reports, you have the option to specify either file-based or time-based selection criteria that determines which CDR records to include.

Use the following procedure to generate a call history report.

Prerequisite

You have Super User [privileges](#) for **Tools** within the **Core Resources** application.

Start

1. Log onto the RAMP GUI.
2. Navigate to **Observability > Tools > Call History**

3. In **Node**, select the SBC Core device whose CDRs you want to include in the call history report.
4. Click **Create Report** to open a window where you can specify selection criteria for the CDRs. You can specify either file-based criteria or time-based criteria.
5. To specify file-based criteria for selecting records, complete the following on the **File Based Search** tab:
 - a. In **Time Span**, select a time range to select a set of CDR records. If needed, click **Show Details** to see the time ranges in a tabular format that is easier to read.
 - b. In **Record Type**, select the type of CDR records to include: **Start**, **Stop**, **Intermediate**, **Attempt**, or **All**.
 - c. In the **Search Criteria** area, use the following table to enter criteria to select CDRs.

Field	Description
Originating Time	The time the call originated.
Disconnect Time	The time the call ended.
Call Duration	The period of time the call was in progress.
Originating Line Info	The originating line information (OLIP), also known as info digits.
Carrier Code	The carrier identification code of the carrier used on the egress trunk (5 characters maximum).
Calling Party Category	A 4-character (8bit hexadecimal code starting with 0x) representing the category of the calling party. For example, 0x0f represents a category of Pay Phone.
Calling Number	The calling number address digits sent out on the egress signaling side after any digit manipulation and address translation performed by the PSX (during the policy request processing) on the calling number received from ingress signaling. (30 characters maximum)
Called Number	The called number address digits sent out on the egress signaling side after any digit manipulation and address translation performed by the PSX (during the policy request processing) on the called number received from ingress signaling. (30 characters maximum)
Dialed Number	The called number digits received by the SBC from the ingress signaling group, before any digit manipulation or address translations are performed by the PSX (30 characters maximum).
Billing Number	One of the following, in order of precedence (30 characters maximum): • the billing number returned by the SCP. • the billing number present in the incoming signaling message. • the billing number configured against the ingress trunk on the PSX.

Field	Description
Ingress TG Name	The origination gateway logs the name of the external trunk group between the ingress network and the origination gateway. The destination gateway logs the name of the internal IP trunk group between the origination gateway and destination gateway.
Egress TG Name	The origination gateway logs the name of the internal IP trunk group between the destination gateway and the origination gateway. The destination gateway logs the name of the external trunk group between the destination gateway and the egress network.
Announcement ID	The 5-decimal digit announcement ID of the last announcement played by the SBC for the call.
Disconnect Reason	The Disconnect Reason code.
Redirecting Number	The redirecting number.
Max. Setup Time	The maximum setup time allowed, in seconds.
Call Answer Time	The time a call was answered (GMT). Click on Select to open a window where you can select the date and time.

- d. (Optional) Click **Include Japanese variants in search** to expand an area where you can enter Japanese variant search options. Use the following table to configure these options.

Field	Description
Called IN Number	The called IN number.
Called Directory Number	The called directory number from the Called Directory Number parameter.

Field	Description
Calling Party Member Status	The Calling Member Status Information in the IAM either received or set after screening is done on the PSX (1 decimal character, 08, or empty). The valid values are: • 0 Pseudo Subscriber • 1 Member • 2 Member (stop service) • 3 Pseudo subscriber (stop service) • 4 Pseudo subscriber (out of service) • 5 Non member • 6 (No definition) • 7 Member1 • 8 Member1 (stop service)
Called Party Member Status	The Called Member Status Information after called member screening is performed (1 decimal character, 08, or empty). The valid values are: • 0 Pseudo Subscriber • 1 Member • 2 Member (stop service) • 3 Pseudo subscriber (stop service) • 4 Pseudo subscriber (out of service) • 5 Non member • 6 (No definition) • 7 Member1 • 8 Member1 (stop service)

- e. In **Display Direction**, select a direction for the report, **Ascending** or **Descending**.
- f. In **Maximum Number of Records**, enter the number of records to include. The maximum allowed is 2048.
6. To specify time-based criteria, specify the following criteria for selecting records on the **Time Based Search** tab:
 - a. In **Record Type**, select the type of CDR records to include: **Start**, **Stop**, **Intermediate**, **Attempt**, or **All**.
 - b. In **Calling Number**, enter a calling number for records to include.
 - c. In **Called Number**, enter a called number for records to include.
 - d. In the **From** and **To** fields under **Call Start Time Range**, click on **Select** to open windows where you can select the beginning and end time for the range of call-start times to include.
 - e. In **Maximum number of records this search will return**, enter the number of records to include. The maximum allowed is 2048.
7. Click **OK** to generate the report.

Call History Settings

When you create a Call History Report, some default settings are specified in the **Ribbon Application Management Platform (RAMP) SystemConfig.txt** file. You can adjust several **systemlevel** parameters in this file to change these defaults. The file resides in the `<BASE_DIR>/weblogic/sonusEMS/data/sys` directory. If you change any parameter values, you must restart RAMP for the changes to take effect.

You can change the following parameters:

Parameter	Default Value	Definition
<code>cdrMaxFiles</code>	32	The maximum number of time spans to list in the Create Call History Report Search window.
<code>cdrMaxRecords</code>	2048	The maximum number of records displayed in a history report.
<code>cdrAlternateExt</code>	ACT	The alternate file extension for CDR files (GSX only).
<code>cdrAlternatePath</code>	N/A	The path to backed-up CDR files (GSX only).
<code>maxNumOfCdrViewer</code>	2	The maximum number of simultaneous Call History sessions allowed.

Note

The `cdrAlternateExt` and `cdrAlternatePath` parameters have no effect if you have configured your GSX(s) to stream CDRs to the DSI.

Inventory

Ribbon Application Management Platform (RAMP) tracks the physical configuration of all registered GSX. Everytime a discovery takes place for a given GSX, RAMP records changes from the previous configuration. RAMP maintains a history of all hardware adds, moves and deletes. The following are examples of some of the reports you can generate:

- The present hardware configuration of a device or of multiple devices
- Configuration changes to a device over a period of time
- The network wide inventory of a particular card type, version, or model number
- The location history of a card with a given serial number
- The software revision of all cards in the network

Note

The list above represents only a small subset of the possible reports.

Prerequisites

- You have Super User [privileges](#) for **Tools** within the **Core Resources** application.
- A GSX device is registered on RAMP.

Start

1. Log onto the RAMP GUI.
2. Navigate to **Observability > Tools > Inventory**.

3. Select a report from the **Reports** drop-down menu. A dialog box displays
4. Select a GSX device from the **Desired GSX Node** drop-down menu.
5. Click the **Create** button to launch the Inventory Reports Wizard.
6. In the **Date Range** window, choose either an inventory snapshot at a specified time, inventory covering a specified range of times, or snapshot of the most recent available inventory information and click **Next**.
7. Select the nodes that you want to inventory. Selecting **All Nodes** includes any new nodes added to the system the next time you run the report template. Click **Next**.
8. Select the modules that you want to include in the inventory. Selecting All Modules includes any new cards added to the system the next time you run the report template. Click **Next**.
9. Select the serial numbers of specific hardware if desired and click **Next**.
10. Select the sort order for the report output and click **Next**.
11. Enter a name for the report and add a description (optional).
12. Select either **Save template and run the report when finished**, **Just save template when finished**, or, **Just run report when finished**. If you select either of the first two options, the report template appears in the Reports pull-down menu for future use.
13. Click **Finish**.

Inventory Reports

Report Name	Description
Latest_All_GSXs	This report shows the most current information on all of the GSX nodes currently configured in the system.
Latest_All_MNS10	This report shows the most current information on all of the MNS10 cards currently installed.
Time_Range_All_GSXs	This report shows information for all GSX nodes over a given time range.
Time_Range_All_MNS10	This report shows information for all MNS10 cards over a given time range.

The following table describes the fields of the Inventory report.

Report Name	Description
GSX Node Name	The name of the GSX containing the server modules.
Inventory reports indicate an unregistered node by placing an asterisk next to the node name.	
Shelf	The shelf number of the GSX
Slot	The slot number of the server module
SubIndex	The index of the CPIM cards in the slot
HW Type	The type of the server module

Report Name	Description
HW Rev	The revision level of the server module
P/N	The Ribbon part number of the server module
P/N Rev	The revision level of the Ribbon part number
Serial #	The serial number of the server module
Inserted Time	The time the system first discovered the server module inserted in the slot

If a server module is present, but not booted, or the HW Type of a server module is unknown, then the P/N, P/N Rev, and Serial # fields will contain the value "N/A".

Report Scheduler

In this section:

- [Report Formats](#)
- [Report Location](#)
- [Report Fields](#)

Ribbon Application Management Platform (RAMP) allows you to schedule generating following reports for GSX devices:

- (Hardware) Inventory (all GSX nodes)
- Blocked ANI (on a selected node)
- Trunk Group reports (all GSX nodes)

After generating the reports, you can save these report locally and forward them to a designated server or location through SCP.

Note

Each report selection results in the generation of a single report containing all information.

When you click on the Report Scheduler, RAMP displays information on all scheduled reports. The start time and frequency settings determine the data selected for a given report. The data contained in (hardware) Inventory reports, Blocked ANI reports, and Trunk Group reports is a snapshot of the applicable records at each designated time interval.

Prerequisites

- You have Super User [privileges](#) for **Tools** within the **Core Resources** application.
- A GSX device is registered on RAMP.

Start

1. Log onto the RAMP GUI.
2. Navigate to **Observability > Tools > Report Scheduler**.
3. Click the **Create** button to open the Create Scheduling Entry dialog box.
4. In the **Report** field, select the type of report to schedule.
 - **Erlang Hourly Data Exporter Report:** The new erlang hourly report generates the report at a scheduled time of the day. The .csv report contains erlang hourly data for previous day from 00:00 hrs to 23:59 hrs. An option is available to generate report for all the GSX devices in the same report or can select report for a selected GSX device.
 - **Erlang Aggregated Data Exporter Report:** The aggregated erlang report scheduled generates a .csv erlang report with a peak erlang usage value, the timestamps when the value was at peak and the average erlang value for the period of 24 hrs, generated at the scheduled time of the day. The report would have report of the previous day. An option is available to generate report for all GSX's together or for one selected GSX device.
5. Perform one of the following as appropriate:
 - If you selected the Blocked ANI report, from the Nodes list, select the name of the node on which you wish to run the report.
 - If you selected either the Trunk Groups or Hardware Inventory reports, the Node field automatically displays All GSXs.
6. In the **Frequency** field, set the frequency (that is, how often you want the system to generate the report) of report generation from the pull-down list of options.
7. In the **Start Time** field, set the day and time for the first report generation. The system generates subsequent reports based upon this start time and the frequency setting.
8. If you wish to save the report file locally, select the **Save to Insight Server Disk** check box.
9. If you wish to transmit the report to a remote location, select the **Save to SCP location** check box, enter the address in the **SCP Hostname** field (for example, *insight.Sonusnet.com.*), the destination directory on the host in the **SCP Directory** field, and enter a valid **User Name** and **Password**. The user name and password must allow read/write access to the specified directory on the remote host.

The acronym, SCP, refers to Secure Copy Program.

10. Click the **Add** button, to add the report destination to the list.

You can add other destinations for the report by repeating Steps 8 and 9. You can modify or delete existing destinations by highlighting the entry and clicking either the Update or Delete buttons.

11. Click **Apply** to save your schedule entry and keep the dialog box open, or click **OK** to save your schedule entry and close the dialog box.

Scheduled Report Fields

Field	Definition
Select	A checkbox used to select the entry for edit or deletion.

Field	Definition
Task ID	The ID of the task of the specific report.
Report	The type of report.
Nodes	A list of the nodes selected for the report.
Frequency	How often the system generates the report. Selectable intervals are: 5 minutes, 15 minutes, 1 hour, 2 hours, 4hours, 6 hours, 12 hours, 1 day, and 1 week.
Next Execution Time	The next execution time based upon the frequency interval and start time. The format is Day, Hours:Minutes AM/PM.
Local	If checked, the system saves a copy of the report locally.
SCP Hostname	The hostname of the system designated for report uploading
SCP Directory	The destination directory for report uploading on the system specified by the SCP Hostname field.

Report Formats

The system generates each report in a comma separated value (.csv) format. The name each scheduled report, whether saved locally or to a remote location, uses the following format:

<Table Name>YYYYMMDDHHMM.csv where YYYYMMDDHHMM represents the time the system created the archive

Example: HW_Inventory2007913530.csv is a hardware inventory report created on September 13, 2007 at 5:30 AM.

or

TrunkGroup20079122148.csv is a trunk group report created on September 12, 2007 at 9:48 PM

Report Headers

Each report contains header information detailing the report type, a report generated timestamp, and field names. Several of the report headers also include a timestamp representing the time of data collection. For example, the header of a Trunk Group report contains a timestamp representing the time the last table synchronization with the GSX occurred. The next section of the report header contains the field names separated by commas. The section that follows the header is the actual report data.

Example (Header form Trunk Group report with excerpt of data)

```
# Trunk Group,2007913956,20079121437
#GroupName,ClusterProfileId,GsxNodeName,Shelf,Slot,Port,Ds3,Ds1,Ds0,T1PortName,TrunkGroup
pName,
```

```

TrunkGroupId,TrunkGroupDescription,TrunkGroupType,TrunkGroupState,TrunkGroupMode,CirResv
State,
PriorityCallReserve,IncomingCallReserve,OutgoingCallReserve,Ds1State,Ds1Mode,Ds0State,Ds
0Mode,
IsupLocalPointCode,IsupRemotePointCode,IsupCic,IsdnChannelType,IsdnInterfaceIdentifier
Default Group,,Demon,1,5,1,0,1,1,T1151,TGISUP1,null,null,ISUP,2, 1,1,1,1,10,2,2,2,2,2530,8
185,0,,
Default Group,,Demon,1,5,1,0,1,2,T1151,TGISUP1,null,null,ISUP,2, 1,1,1,1,10,2,2,2,2,2530,8
185,6,,
Default Group,,Demon,1,5,1,0,1,3,T1151,TGISUP1,null,null,ISUP,2, 1,1,1,1,10,2,2,2,2,2530,8
185,12,,
Default Group,,Demon,1,5,1,0,1,4,T1151,TGISUP1,null,null,ISUP,2, 1,1,1,1,10,2,2,2,2,2530,8
185,18,,

```

Report Location

When you select the option, Save to local disk, the system saves each report to a directory specified in the `SystemConfig.txt` file.

The default locations are as follows:

Default Report Location

Report Type	Location
Hardware Inventory for all GSXs	<BASE_DIR>/weblogic/sonusEms/data/ HwInventoryReports
Blocked ANI Data Exporter	<BASE_DIR>/weblogic/sonusEms/data/ blockedANI_archive/<node name>
Trunkgroups for all GSXs	<BASE_DIR>/weblogic/sonusEms/data/ TrunkGroupReports
Erlang Hourly Data Exporter	<BASE_DIR>/weblogic/sonusEms/data/ ErlangHourlyReports
Erlang Aggregated Data Exporter	<BASE_DIR>/weblogic/sonusEms/data/ ErlangAggregatedReports

To change the default locations, edit the following parameters in the `SystemConfig.txt` file:

- `hwInventoryExportDir=<your new path>`
- `blockedAniExportDir=<your new path>` (Do not include the node name.)
- `trunkgroupExportDir=<your new path>`
- `erlangHourlyExportDir=<your new path>`
- `erlangAggregatedExportDir=<your new path>`

Note

Report files are not replicated for any reports in a Disaster Recovery set up.

If you wish to export reports to a single location (or both), use SCP option and add both DR Source and Target as export locations. You can also export to a third server from both Source and Target.

Report Fields

The following table supply definitions for the various fields contained in the reports you can generate using the Report Scheduler.

Note

Inventory reports indicate an unregistered node by placing an asterisk next to the Node Name.

Hardware Inventory Report Fields

Field	Description
groupName	The name of the device group to which the GSX belongs
CLUSTER_PROFILE_ID	The ID of the Cluster Profile to which the GSX belongs as defined in the GATEWAY table of the PSX.
gsxNodeName	The name of the GSX containing the server modules
SwRevision	The version of the software on the GSX. For example, V07.01.00R000
Shelf	The shelf number of the GSX
Slot	The slot number of the server module

Field	Description
HW Type	The type of the server module. The values are defined as follows: • none = 1 • UNIX = 2 • CUPSS02 = 12 • CUPSS01= 13 • MIN = 14 • VME = 15 • MNS10 = 16 • PNS10 = 17 • CNS10 = 18 • CNS30 = 19 • MTA01 = 20 • MNA10 = 21 • PNA10_QUAD = 22 • CNA33 = 23 • CNA10 = 24 • CNA30 = 25 • SONICPLANE01 = 26 • FANTRAY01 = 27 • MTA10 = 28 • CNA01 = 29 • CNA03 = 30 • CNS20 = 31 • PNS20 = 32 • SPS60 = 33 • CNA20 = 34 • CNA21 = 35 • PNA21 = 36 • PNA23 = 37 • CNS61 = 38 • CNA61 = 39 • MTA20 = 40 • MTA21 = 41 • CNA06 = 42 • CNS31 = 43 • CNS25 = 44 • CNA25 = 45 • PNS30 = 46 • PNA30 = 47 • SONICPLANE02 = 48 • CNA02 = 49 • CNA05 = 50 • CNS60 = 51 • CNS70 = 52 • CNA60 = 53 • CNA70 = 54 • CNA07 = 55 • CPIM70 = 56 • CPIM71 = 57

Field	Description
	• MNS11 = 58 • MTA30 = 59 • CNS71 = 60 • SPS70 = 61 • CNA73 = 62 • PNA35 = 63 • MNS20 = 64 • MNA20 = 65 • MNA21 = 66 • MNA25 = 67 • MNS25 = 68 • PNS40 = 69 • PNS41 = 70 • PNA40 = 71 • PNA41 = 72 • PNA45 = 73 • GNS15 = 74 (GSX4010) • GNA10 = 75 (GSX4010) • FMP10 = 76 (GSX4010) • GNS16 = 77 • GNS30 = 78 • GNA30 = 79 • FMP30 = 80 • GCA30 = 81 • GCA31 = 82 • GNS31 = 83 • GNS35 = 84 • GNS36 = 85 • CNS40 = 86 • CNS45 = 87 • CNS80 = 88 • CNS81 = 89 • CNS85 = 90 • CNS86 = 91 • SPS80 = 92 • CNA40 = 93 • CNA80 = 94 • CNA81 = 95 • CPIM81 = 96 • CNA08 = 97 • CNA04 = 98 • MNS21 = 99 • MNS26 = 100
HW Rev	The revision level of the server/adaptor module

Field	Description
Server or Adaptor	Defines whether the server module is a server or adaptor module. Possible values are: • Server = 1 • Adaptor = 2 • MTA = 3 • CPIM = 4
P/N	The Ribbon part number of the server module
P/N Rev	The revision level of the Ribbon part number
Serial #	The serial number of the server module
Inserted Time	The time the system first discovered the server module inserted in the slot
Sub-Index	1 for upper CPIM71 or CPIM81 and 2 for lower CPIM71 or CPIM81 and 0 for all other hardware types.

Note

The following cards are not supported ; MNS11, PNS10, PNS20, PNS30, PNS30a, CNS10, CNS25, CNA01, CNA02, CNA05, CNA10, CNA20, CNA21, CNA25, CNS30, CNS30a, CNS31, CNA33, MNS10, MNA10, PNA10, CNA30, CNA03, CNS20, SPS60, PNA21, PNA23, CNS61, CNA61, CNA06, PNA30, CNS60, CNS70, CNA70, CNA07, CPIM70, CPIM71, CNS71, SPS70, CNA73, PNA35, MNS20, MNS25, PNS40, PNA41.

Trunkgroup (Details) Report Fields

Field	Definition
groupName	The name of the device group to which the GSX belongs
ClusterProfileId	The ID of the Cluster Profile to which the GSX belongs as defined in the GATEWAY table of the PSX.
gsxNodeName	The name of the GSX containing the server modules
Shelf	The shelf number of the GSX
Slot	The slot number of the server module
Port	The Port index

Field	Definition
Ds3	The DS3 index
Ds1	The DS1 index
Ds0	The DS0 index
T1PortName	The name of the port
TrunkGroupName	The name of the trunk group (Trunkgroup CLI)
TrunkGroupID	The ID of the trunkgroup as defined in the TRUNKGROUP_ID2 field of the PSX TRUNKGROUP table.
TrunkGroupDescription	Description text for the trunkgroup as entered in the DESCRIPTION field of the PSX TRUNKGROUP table.
TrunkGroupType	The trunkgroup type. Possible values are: ISUP, CAS, or ISDN.
TrunkGroupState	The administrative state of the trunkgroup. Possible values are: 1 if disabled, or 2 if enabled. All trunk groups are created in a disabled state and must be enabled to allow calls.
TrunkGroupMode	Operation mode for this trunkgroup. Possible values are: 1 for inService, or 2 for outOfService.
CirResvState	The administrative state of the circuit reservation feature on the trunk group. Possible values are: 1 if disabled, or 2 if enabled. All trunk groups are created with this feature in a disabled state. If you enable this feature, then the SonusTgInboundReserved feature is overridden.
PriorityCallReserve	Minimum number of priority call allowed set for this trunk group when SonusTgCirResvState is set to enabled. Possible values: Integer in the range of 0 to 100.
IncomingCallReserve	Minimum number of incoming call allowed set for this trunk group when SonusTgCirResvState is set to enabled. Possible values: Integer in the range of 0 to 128.
OutgoingCallReserve	Minimum percent of outgoing call allowed set for this trunk group when SonusTgCirResvState is set to enabled. Possible values: Integer in the range of 0 to 100.

Field	Definition
Ds1State	The administrative state of this T1/E1 span. Possible values are: 1 for disabled, 2 for enabled, 3 for deleted, 4 for inservice, or 5 for dryingUp.
Ds1Mode	The service state of this T1/E1 span. Possible values are: 1 for outOfService, or 2 for inService.
Ds0State	The administrative state of this DS0 channel. Possible values are: 1 for unavailable, or 2 for available.
Ds0Mode	The service state of this DS0 channel. Possible values are: 1 for outOfService, or 2 for inService.
IsupLocalPointCode	The SS7 point code assigned to this SS7 Node for the gateway. Format: three octet data type representing NetworkClusterMember values respectively. Applicable only to ISUP trunk group type. Set to 0 for other (CAS and ISDN) trunk group types. Integer value with range of 0 to 16777215.
IsupRemotePointCode	The SS7 Point Code of the ISUP Service Group in decimal format, the least significant three bytes representing NetworkClusterMember values. Set to 0 for CAS and ISDN trunk group types.
IsupCic	Identifies the circuit identity code (CIC) for the ISUP circuit. Integer values in the range 0 ... 16383. Set to 0 for CAS and ISDN trunk group types.
IsdnChannelType	The ISDN channel type. Possible (integer) values: 1 for ISDN B Channel, 2 for ISDN Primary D Channel, or 3 for Backup D Channel
IsdnInterfaceIdentifier	The Q931 interface identifier of the ISDN Service Group interface.

Trunkgroup (Summary) Report Fields

Field	Definition
groupName	The name of the device group to which the GSX belongs
ClusterProfileId	The ID of the Cluster Profile to which the GSX belongs as defined in the GATEWAY table of the PSX.
gsxNodeName	The name of the GSX containing the server modules
TrunkGroupName	The name of the trunk group (Trunkgroup CLLI)

Field	Definition
TrunkGroupID	The ID of the trunk group as defined in the TRUNKGROUP_ID2 field of the PSX TRUNKGROUP table.
TrunkGroupDescription	Description text for the trunkgroup as entered in the DESCRIPTION field of the PSX TRUNKGROUP table.
TrunkGroupState	The administrative state of the trunk group. Possible values are: 1 if disabled, or 2 if enabled. All trunk groups are created in a disabled state and must be enabled to allow calls.
TrunkGroupMode	Operation mode for this trunk group. Possible values are: 1 for inService, or 2 for outOfService.
CirResvState	The administrative state of the circuit reservation feature on the trunk group. Possible values are: 1 if disabled, or 2 if enabled. All trunk groups are created with this feature in a disabled state. If you enable this feature, then the SonusTgInboundReserved feature is overridden.
PriorityCallReserve	Minimum number of priority call allowed set for this trunk group when SonusTgCirResvState is set to enabled. Possible values: Integer in the range of 0 to 100.
IncomingCallReserve	Minimum number of incoming call allowed set for this trunk group when SonusTgCirResvState is set to enabled. Possible values: Integer in the range of 0 to 128.
OutgoingCallReserve	Minimum percent of outgoing call allowed set for this trunk group when SonusTgCirResvState is set to enabled. Possible values: Integer in the range of 0 to 100.
TotalConfiguredDSOs	The sum of all configured and registered PSTN channels for this trunk group. This number is obtained from the SonusTgPstnTotalConfigured field of SonusTgStatusTable MIB table. Consequently, to get correct values, you must enable performance data collection for all nodes.

Field	Definition
TotalEnabledDSOs	Current effective number of DSOs enabled. This count more correctly reflects the effective enabled DSOs channel count, based on whether the channels are being used for call handling. Consequently, to get correct values, you must enable performance data collection for all nodes. This number is the sum of the following fields of the SonusTgStatusTable MIB table: • SonusTgPstnTotalAvailable — The sum of all available or unblocked PSTN channels for this trunk group. • SonusTgPstnInboundUsage — This is only meaningful for PSTN trunk groups that are configured for inbound or both directions. This reflects the current inbound or incoming usage count of this trunk group. • SonusTgPstnOutboundUsage — This is only meaningful for PSTN trunk groups that are configured for outbound or both directions. This reflects the current outbound, outgoing or nonpriority usage count of this trunk group. • SonusTgPriorityCallUsage — This is only meaningful for ISUP trunk groups that are configured and when SonusTgCirResvState is enabled. This reflects the current priority usage count of this trunk group.

Blocked ANI Report Fields

Field	Definition
Automatic Number ID	The ID of the blocked subscriber.
Blocked Reason	The reason for the block either Access, or Fraud

Trunk Group

In this section:

- [Trunk Group Reports](#)
- [Trunk Group Report Fields](#)
- [Trunk Group Wizard Profile](#)
- [Trunk Group Wizard for PSX](#)
- [Trunk Group Wizard ISUP Service Group](#)
- [Trunk Group Wizard CIC](#)

Related articles:

- [Renaming Trunk Groups](#)

Ribbon Application Management Platform (RAMP) supports generating Trunk Groups reports.

The Trunk Group Wizard provides a centralized mechanism for the creation of trunk groups and supporting entities across the Ribbon platform (GSX, PSX, and SGX nodes).

For more information on GSX trunk groups, refer to [Trunk Group](#).

Prerequisites

- Super User [privileges](#) for **Tools** within the **Core Resources** application.
- GSX Super User privileges for creating a task list using the Trunk Group Wizard (a minimum level of GSX Provisioner to run the task list). The system disables access to the Trunk Group Wizard for users with lower privilege levels.
- PSX read/write privileges for the PSX Trunk Group to access the PSX configuration section of the Trunk Group Wizard.
- A GSX device is registered on RAMP.
- Before you can successfully employ the Trunk Group Wizard to create ISUP trunk groups, you must create and configure the following objects on the GSX and the PSX:
 - At least one Carrier on the GSX
 - At least one SS7 node on the GSX
 - At least one CNS server on the GSX
 - (If you plan to create the trunk group on a PSX) The PSX on the GSX the PSX must be a registered node in **RAMP** with the same name
 - (If you plan to create the trunk group on a PSX) A Carrier with the same ID (as on the GSX) must exist on the PSX
 - Enable Data Collection for the GSX (enabling incremental PIF recommended) and verify data collection is up-to-date.

Start

1. Log onto the [RAMP](#) GUI.
2. Navigate to **Observability > Tools > Trunk Group**.
3. Select a report from the **Reports** drop-down menu. A dialog box displays
4. Select a GSX device from the **Desired GSX Node** drop-down menu.
5. Click **OK**. The report displays.

Trunk Group Reports

Node Object	Report (Command)
Shelf, Hardware, CNS/CNA, GNS/GNA, and Port	• Report Dependent Trunk Groups Detail • Report Dependent Trunk Groups Summary • Report Unassigned Channels Detail • Report Unassigned Channels Summary • Report Used Channels Detail
Trunk Group(s)	• Report Unassigned CICs • Report Used CICs Summary • Report Used Channels • Report Used Channels Detail • Report Used Ports • Report Used Slots

The header of each report contains general information about the report (that is, Report Name, Node, Report Generation (date), Data Collected (date), etc.). Report for a single GSX trunk group or a consolidated report for all the GSXs in the entire network can be generated.

Trunk Group Report Fields

Report Name	Field/Definition
Dependent Trunk Groups Detail	• Slot — The chassis slot where the server module resides • Port — Assigned name of the port. Syntax is TypeShelfSlotIndexSpan (for example, T11815) • Trunk Group — The name assigned to the Trunk Group • Trunk Group Type — The Trunk Group type (that is, ISUP, ISDN, etc.) • Channels — Number of channels on the span
Dependent Trunk Groups Summary	• Slot — The chassis slot where the server module resides • Trunk Group — The name assigned to the Trunk Group
Unassigned Channels Detail	• Slot — The chassis slot where the server module resides • Port — Assigned name of the port. Syntax is TypeShelfSlotIndexSpan (for example, T11815) • Unassigned Channels — The channel number(s) of unassigned channels on the span
Unassigned Channels Summary	• Slot — The chassis slot where the server module resides • Number of Unassigned Channels — The quantity of unassigned channels associated with the server module in the designated slot
Used Channels Detail	• Trunk Group — The name assigned to the Trunk Group • Trunk Group Type — The Trunk Group type (that is, ISUP, ISDN, etc.) • Port — Assigned name of the port. Syntax is TypeShelfSlotIndexSpan (for example, T11815) • Slot — The chassis slot where the server module resides • Channel — The channel number on the span • LPC — The local point code of the ISUP circuit • LPC (Decimal) — The local point code of the ISUP circuit in decimal format • RPC — The remote point code of the ISUP circuit • RPC (Decimal) — The remote point code of the ISUP circuit in decimal format • CIC — The circuit identifier of the ISUP circuit • ISDN Channel Type — The ISDN channel type • ISDN Interface ID — The ISDN interface identifier

Report Name	Field/Definition
Unassigned CICs and Used CICs Summary	• Trunk Group — The name assigned to the Trunk Group • Trunk Group Type — The Trunk Group type (that is, ISUP, ISDN, etc.) • LPC — The local point code of the ISUP circuit • LPC (Decimal) — The local point code of the ISUP circuit in decimal format • RPC — The remote point code of the ISUP circuit • RPC (Decimal) — The remote point code of the ISUP circuit in decimal format • CICs — The range of circuit identifiers of the ISUP circuit
Used Channels	• Trunk Group — The name assigned to the Trunk Group • Trunk Group Type — The Trunk Group type (that is, ISUP, ISDN, etc.) • Port — Assigned name of the port. Syntax is TypeShelfSlotIndexSpan (for example, T11815) • Slot — The chassis slot where the server module resides • Channels — Number of channels on the span
Used Ports	• Trunk Group — The name assigned to the Trunk Group • Slot — The chassis slot where the server module resides • Ports Used — a list of the physical ports used by this Trunk Group
Used Slots	• Trunk Group — The name assigned to the Trunk Group • Slots Used — The chassis slot (location of the server module) used for this Trunk Group

Trunk Group Wizard Profile

Carrier Name and SS7 Node Name are mandatory fields. The listed carriers may change depending upon whether you selected to skip the PSX trunk group creation. If you selected the **Skip PSX Trunk Group Creation** check box, then the carriers listed are those configured on the GSX. If you did not select the **Skip PSX Trunk Group Creation** check box, then the carriers listed are those common to both the GSX and the PSX.

Field	Definition
Existing Profile (optional)	Selection of an existing Trunk Group profile populates the required fields with information from the profile. You may override any of this information by changing the field value.
Carrier Name (required)	Select the carrier associated with the trunk group. The carrier must exist on both the GSX and the PSX Policy Server (unless you disabled the PSX configuration see Note above).
SS7 Node Name (required)	Select the name of the SS7 Node that provides SS7 signaling for the trunk group.

Field	Definition
Inbound Reserve (%) (optional)	Specifies the percent of channels reserved for inbound calls in PSTN trunk groups. (Defined in increments of 5. Default = 0) If enabled, the Circuit Reserve State overrides this parameter.
Mode (optional)	Defines if the trunk group will be in service or out of service after creation. • inService • outOfService
Num Verify	Specifies whether the Trunk Group may require verification for the calling number.
Num 800	Specifies whether the Trunk Group may require 800 number translation for the called number.
Priority Call Reserve (%) (optional)	Specifies the percent of channels reserved for priority calls in PSTN trunk groups. (Defined in increments of 5. Default = 0). The system uses this parameter only if the Circuit Reserve state is enabled.
Incoming Call Reserve (%) (optional)	Specifies the percent of channels reserved for incoming calls in PSTN trunk groups. (Defined in increments of 5. Default = 0). The system uses this parameter only if the Circuit Reserve state is enabled.
Outgoing Call Reserve (%) (optional)	Specifies the percent of channels reserved for outgoing calls in PSTN trunk groups. (Defined in increments of 5. Default = 0). The system uses this parameter only if the Circuit Reserve state is enabled.

Field	Definition
Circuit Reserve State (optional)	If the Circuit Reserve State is enabled then system ignores the Inbound Reserve parameter and uses the Priority, Incoming, and Outgoing Call Reserve parameters. If disabled, the system uses the Inbound Reserve parameter.
Hunt Method (required)	The method of hunting through service groups for trunk groups: • leastcost — examines the leastcost service group first, then the next least etc. • configured — examines the first configured service group first, then the second, etc. • circularforward — the search for an available resource proceeds through all service groups in the order that they registered to the trunk group. This selection overrides the hunt method for the service group. • circularbackward — the search for an available resource proceeds through all service groups in the opposite (reverse) order that they registered to the trunk group. This selection overrides the hunt method for the service group
LNP Trans	Select True or False
SILC Cong. Level 1 Calls Allowed	The percentage of call to allow when the first congestion level trigger is surpassed. This should be set to a higher value than the Level 2 Calls Allowed setting.
SILC Cong. Level 2 Calls Allowed	The percentage of call to allow when the second congestion level trigger is surpassed. This should be set to a lower value than the Level 1 Calls Allowed setting.
SILC State	The state of the Selective Incoming Load Control either Disabled or Enabled .

Trunk Group Wizard for PSX

If you selected the **Skip PSX Trunk Group Creation** check box on the first wizard window, then the wizard does not display this window. Go to the Fourth Window: ISUP Service Groups.

You can use this window to enter PSX related trunk group information. There are no mandatory parameters. However, you may wish to populate many of the optional fields. The following table provides information about the optional fields.

Field	Definition
Unrestricted Flag (optional)	Indicates if this trunk group may carry 64 kbps clearchannel data call or is restricted to 56 kbps
Gateway (required)	The name of the GSX node to which this trunk group belongs.

Field	Definition
Description (optional)	An optional description of the trunk group.
Business Group (optional)	The ID of the business group assigned to this trunk group.
Business Location (optional)	The ID of the business location assigned to this trunk group. • Generic • JAPAN • North America • Unknown
Calling Area	The calling area in which this trunk group is located. Used for local call determination and AMA billing.
Call Processing Localized Variant (optional)	This field defines the PSX Call Processing Localized Variant to use for this trunk group.
PSX Carrier	Not editable. Populated from selection in previous window.
Carrier Selection Priority (optional)	The carrier selection priority used for this trunk group.
Country (optional)	The country code of the country at the far-end of the trunk group.
Destination Switch Type (required)	Identifies the far end switch type connected to this trunk group. Possible selections are: • Access • Tandem • EAEO • nonEAEO • IXC • International
Direction (required)	Indicates which call directions are allowed on this trunk group. This setting must match the setting for the trunk group members (ISUP circuits) provisioned on the GSX. • Unknown • Two Way Allows both inbound and outbound • One Way In Allows inbound calls only • One Way Out Allows outbound calls only.
Element Routing Priority Profile (optional)	The Element Routing Priority profile used for outgoing calls on this trunk group. • DEFAULT • JAPAN • NA

Field	Definition
Feature Control Profile (required)	The feature control profile to use for this trunk group.
LATA (optional)	The LATA that contains the far end of the trunks in this trunk group. Outside North America, the LATA you choose has no effect on calls.
Max. Satellite Hops	Specifies the maximum number of hops allowed for a trunk group designated as a satellite trunk group. Possible values are: • None • One Hop • Two Hops • Three or more Hops
Numbering Analysis Profile (optional)	Specifies the number analysis profile for this trunk group.
Number Length Enforcement (optional)	The number length enforcement entry for this trunk group.
Originating Carrier (required)	The carrier code of the carrier owning the CO switch at the far end of the trunks in this group.
PPR Profile (optional)	The ID of the Prefix Partition Routing Profile assigned to this trunk group.
Pseudo Carrier (required)	The subscriber's assigned carrier. Use this field when the subscriber belongs to a carrier that does not have a CIC, or when the subscriber belongs to a reseller.
Routing Criteria Profile (optional)	The Routing Criteria priority profile used for outgoing calls on this trunk group.
SCP Business Service Group (0255) (required)	The SCP Business Service Group associated with the trunk group.
Signaling Profile (optional)	The Signaling Profile specifies outgoing signaling parameters overriding the default behavior directed by the signaling flag.
Signaling Flag (required)	The type of call control signaling used to set and tear down calls on this trunk group.
SIP Domain (optional)	The regional domain name assigned to this trunk group.
TDM Trunk Type (required)	Defines the type of TDM trunks.

Field	Definition
Trunk Group Class of Service (optional)	The trunk group class of service (COS) associated with this trunk group. Either an Egress COS or Ingress COS that you previously define in the Trunk Group COS Profile.
Trunk Group Class of Service Profile (optional)	The associated Trunk Group COS Profile. Select a Trunk Group COS Profile for ingress trunk groups only.
Trunk Group Domain (optional)	The default domain to use for this trunk group if no other domain is specified.
Trunk Number (optional)	The five digit trunk number.
ZZ Profile (optional)	The ZZ profile to be used for outgoing calls on this trunk group. This applies to channel associated signaling (CAS) trunk groups only.
POI Level (required)	Specifies the Point of Interface (POI) Level. • 0 – The Trunk Group does not have multiple POI levels • 1 – PSX Fixed Services (for carriers with more than one POI level) • 2 – Mobile Services (for carriers with more than one POI level)
POI Charge Area (optional)	The Point of Interface (POI) Charge Area represents the point of demarcation between two carriers. If the PSX does not find the HNPA Charge Area Code during pre-routing, it uses this value to determine the Charge Area Code for the called or calling number.
Own Carrier ID	The carrier code of the carrier used as the call carrier if Carrier Selection Priority indicates Trunk Group as the source.
Release Tone Treatment (0999)	Not used in this release. Enter 0.
NOA Profile (optional)	The Nature of Address profile.
Prefix Profile (optional)	The Prefix Profile for this trunk group.
Owning Carrier Profile ID (optional)	(Japan variant only) The profile defines the owning carrier for certain calling and called numbers or number prefixes on this trunk group.
Carrier Type Profile (optional)	(Japan variant only) When provisioned, the PSX determine the carrier type based on the call type, ingress destination switch type, and egress destination switch type.

Field	Definition
Ingress Charge Indicator (required)	Defines if there is a charge associated with the call. Possible values: • None Used for backward compatibility or test calls with no charge indicator. • No Charge The call is not charged. • Charge The call is charged.
Default CPC (optional)	The default Calling Party Category to use for this trunk group
Default OLIP (0255) (required)	The default Originating Line Information Parameter digits (Infodigits) to associate with calls coming from this trunk group when the inbound call IAM message does not contain an OLIP value. This indicates the call source (prison, payphone, etc.) to upstream switches.
Dial Plan Profile (optional)	The dial plan profile used for this trunk group. Use this profile to enforce standard dialing rules.
In DM/PM Rule (optional)	Digit manipulation/Parameter manipulation rule applied to the calling party and/or called party digits when calls for calls received on this trunk group.
JIP (required)	The default Jurisdiction Information Parameter for this access trunk group. This defines the jurisdiction (NPANXX) of the trunk group to upstream switches, and applies only to Access trunks. If this is not an Access trunk group, enter 0.
NPA (required)	Default NPA applied to called numbers received on this trunk group. The system applies this only if the IAM message does not contain an NPA (for example, in 7digit dialing scenarios).
Numbering Plan (optional)	The numbering plan used for calls originating on this trunk group. The PSX includes two pre-populated numbering plans to select from or you can define your own: • NANP_ACCESS—Use this numbering plan if the calls that originate on this trunk group are North American calls (for example, if this trunk group is connected to a PBX and the PSX performs North American digit analysis of the called and calling numbers). • NANP_IXC—Use this numbering plan if calls originating on this trunk group are IXC calls (for example, if the trunk group is connected to another switch which has already performed North American digit analysis). • User Defined
Overlap Dialing (optional)	Select to enable overlap dialing on this trunk group

Field	Definition
TNS Circuit Code Based Routing (optional)	Select the check box to enable Transit Network Selection (TNS) circuit-based routing on this trunk group. If G.394 signaling is used, the TNS parameter is sent in the signaling. The TNS parameter includes the circuit code. The circuit code contains information that identifies a call as an international call or other network specific call type. The far-end IXC switch can perform routing based on the TNS parameter.
Egress Charge Indicator (optional)	See Charge Indicator
Out DM/PM Rule (optional)	The outbound digit manipulation/parameter manipulation rule applied to the calling party and/or called party digits before the system routes calls out on this trunk group.
Billing Plan (optional)	The Billing Plan for this trunk group.
Billing Information (optional)	The Billing Profile for this trunk group.
Default Billing Number (optional)	The Billing Number for this trunk group.
Billing NOA (required)	The Nature of Address used when the PSX derives the Billing Number from the trunk group.
Billing NPI (required)	The Numbering Plan Indicator to be used when the system derives the Billing Number from the trunk group.
Calling Party (optional)	The default calling party number for calls originating on this trunk group. The PSX uses this value only if the IAM message does not provide the calling party number.
Calling Party NOA (required)	The Nature of Address when the system derives the Calling Party Number from the trunk group.
Calling Party NPI (required)	The Numbering Plan Indicator used when the system derives the Calling Party Number from the trunk group.
CPN Presentation (required)	Specifies the presentation method used for the calling party number (CPN) for calls originating on this trunk group. • None • Allowed • Number Unavailable • Restricted • Spare

Field	Definition
CPN Screening (required)	Specifies the screening method used for the calling party number (CPN) for calls originating on this trunk group. • None • Network Provided Not Screened • User Provided Failed Network Screening • User Provided Not Screened • User Provided Passed Network Screening
Default CPN Presentation (required)	Specifies the default presentation method used for the calling party number (CPN) for calls originating on this trunk group. • None • Allowed • Number Unavailable • Restricted • Spare
Business Group from CLI (Calling Line ID) (optional)	If selected, the PSX obtains the business group ID from the calling line identification (CLID) number provisioned on the Business Group Subscriber screen for calls from business group subscribers received on this ingress trunk group
Out of Service (optional)	Select the check box to take this trunk group out of service for egress of calls. In particular, if this check box is selected, the PSX deletes any route which includes this Trunk Group from the list of returned routes.
Do Not Use Fallback Bearer Capability (optional)	If selected, the PSX does not use this trunk group for fallback routing.
Satellite Trunk	Use this flag to designate this trunk group as a satellite trunk group.
Escaped (optional)	Specify if you wish to designate this trunk group as an escaped trunk group.
Preferred Packet Service Profile (optional)	The preferred packet service provider assigned to this trunk group.
Destination Override	Packet service profile destination override check box: • Selected—The PSX uses the egress (destination) trunk group's packet service profile. • Cleared—The PSX uses the ingress (originating) trunk group's packet service profile.

Field	Definition
Trunk Group Reservation Level 1 (optional)	When congestion has reduced number of free circuits to this setting, the system automatically applies the Selective Trunk Reservation (STR) control designated for this level.
Trunk Group Reservation Level 2 (optional)	See Trunk Group Reservation Level 1 above.
Screening	Defines the type of screening. Select one of the following: • Not Screened • Screened Normal • Screened Fraud
Class of Service ID (optional)	Enables you to select a trunk group class of service (COS).
Exception Profile (optional)	The Exception Profile for this trunk group.

Trunk Group Wizard ISUP Service Group

You use this window to enter information related to the creation of an ISUP service group on the GSX. If you previously created an ISUP Service Group Profile on the GSX, you can select it from the list box and wizard populates the field values with the values from the profile. You can override any profile setting by changing the value in that field. The following table provides information about the fields in this window.

Field	Description
Existing Profile (optional)	Select an existing Service Group Profile
Service Group Name (required)	Assign a name to the Service Group.
Destination PC (required)	The destination point code of the central office switch connected to this service. The range of legal values for this triplet depends upon the revision of ISUP protocol supported by this service: • ANSI1992 and ANSI1995 (0255)(0255)(0255) The field length is 8bits8bits8bits for this protocol. • ITU and ETSI2 (07)(0255)(07) The field length is 3bits 8bits 3bits for this protocol. The DPC format in the ISUP Service Group must match the LPC format of the selected SS7 node.
Operation Mode	The operational state of the ISUP service: The system automatically sets this field to in service and can not be edited.
Signaling Profile (optional)	The name of the ISUP signaling profile to apply to this ISUP service.

Field	Description
Proto Revision (optional)	The ISUP protocol revision supported for this ISUP service: Options are: • ansi1992 Use this protocol if this ISUP service connects to either a dms or an ess SWITCHTYPE. • ansi1995 • ansiatt • argentina • argentinaidt • belgacom • brazil • chile • chinacnc • denmarkic • etsi2 use for Germany and Netherlands • etsi2plus • etsi3 • hongkongic • india • israel • italy • itu1988 • itu1993 • itu1997 • ituq767 Same as etsii (has been renamed) • korea • mexicoic • nttcom NTT Communications protocol for Japan • nttfcc For Japan • portugaloni • singapore • spain • spirou • ukisup
Hunt Algorithm (optional)	The hunting method used to select circuits for calls to the Service Group destination. Possible values are: • bottom2top • top2bottom • circuiti2lo • circuitlo2hi • mostnleastidle • circularbottom2top • circulartop2bottom
Relative Cost (optional)	The relative cost of using the CICs configured in this service. Valid values are between 0 and 100, where a value of 100 represents the highest possible cost.

Field	Description
CIC Control (optional)	The set of CICs controlled by this GSX for the sake of resolving dualseizure scenarios. Additionally, if the HUNT parameter is set to mostnleasidle, a CIC search algorithm is also implied. • nocics — This GSX does not control the CICs in the service group. If HUNT is mostnleasidle, CIC hunting is LastInFirstOut (LIFO). • allcics — The GSX controls all CICs in the service group. If HUNT is mostnleasidle, CIC hunting is FirstInFirstOut (FIFO). • oddcics — The GSX controls odd numbered CICs (1,3,5, etc.) in this service group. If HUNT is mostnleasidle, these CICs are hunted FIFO while even numbered CICs are controlled by the remote switch and hunted LIFO. • evencics — The GSX controls even numbered CICs (2,4,6 etc.) in this service group. If HUNT is mostnleasidle, these CICs are hunted FIFO while odd numbered CICs are controlled by the remote switch and hunted LIFO
Continuity Test Frequency (optional)	Identifies the frequency of continuity test performed on each circuit. Options are: • 0 do not perform continuity test • 1 perform continuity test per call • 2 to 16 perform continuity test every nth call
Hop Count Value (required)	Defines the Hop Count Value. You must set the Hop Count State to enabled for this parameter to apply. (Valid values are between 10 and 32.) If you set a Hop Count Value, you should set the Hop Count State to enabled.
Switch Type (optional)	Defines the type of central office switch connected to this service. Options are: • lucent4ESS • lucent5ESS • dms100 • dms200 • dms250 • dms500

Field	Description
Hop Count State (optional)	Defines the Hop Count State for the Service Group. Options are: • enabled — The procedures are in effect. This state requires that the ISUP protocol revision be ANSI1992 or ANSI1995. • disabled — The procedures are not in effect. When Hop Counting is enabled: • If the GSX receives a Hop Counter parameter from the ingress leg of the call, the GSX decrements and includes the count in the outgoing IAM message. If the GSX does not receive a Hop Counter in the ingress leg of the call, the GSX includes a value in the outgoing IAM message based upon the setting in the Hop Count Value field. • If the GSX receives a Hop Counter value of zero in the ingress leg of the call, the GSX releases the call with a cause of "exchange routing error". When Hop Counting is disabled: • If the GSX receives a Hop Counter parameter from the ingress leg of the call, the GSX passes it transparently in the outgoing IAM message. • If the GSX receives a Hop Counter value of zero in the ingress leg of the call, the GSX releases the call with a cause of "exchange routing error"
Disconnect Treatment Profile (optional)	Defines the Disconnect Treatment Profile used to map a disconnect reason code to a Disconnect Signaling Sequence Profile (SSP) for the ISUP service.
Tone Package (optional)	The name of a tone package used by the ISUP service.
GRS at Startup (optional)	Specifies whether to issue the GroupReset (GRS) message on all circuits when initializing the CNS module. All circuits that belong to the ISUP service controlled by the module receive the GRS message. If GRS is not supported, individual RSC messages will be issued on CNS restart. • unsupported — do not issue the GRS message on startup • supported — issue the GRS message on startup
Exchange Type (optional)	Specifies the Exchange Type to which this service applies: • none • typeA — single user services. • typeB — services that affect multiple users
Acc L1 AR Cancel (%) (optional)	Defines the Automatic Congestion Control (ACC) Level 1 (L1) Alternate Routed (AR) Cancel Percentage. If a congested condition occurs, the GSX releases this percentage of alternaterouted calls.

Field	Description
Acc L1 DR Cancel (%) (optional)	Defines the Automatic Congestion Control (ACC) Level 1 (L1) Direct Routed (DR) Cancel Percentage. If a congested condition occurs, the GSX releases this percentage of directrouted calls. A direct routed call is a call that first arrives to a service group for routing, but the GSX has not attempted a retry.
Acc L2 AR Cancel (%) (optional)	Defines the Automatic Congestion Control (ACC) Level 2 (L1) Alternate Routed (AR) Cancel Percentage. If a congested condition occurs, the GSX releases this percentage of alternaterouted calls.
Acc L2 DR Cancel (%) (optional)	Defines the Automatic Congestion Control (ACC) Level 2 (L1) Direct Routed (DR) Cancel Percentage. If a congested condition occurs, the GSX releases this percentage of directrouted calls. A direct routed call is a call that first arrives to a service group for routing, but the GSX has not attempted a retry.
Acc L3 AR Cancel (%) (optional)	Defines the Automatic Congestion Control (ACC) Level 3 (L1) Alternate Routed (AR) Cancel Percentage. If a congested condition occurs, the GSX releases this percentage of alternaterouted calls.
Acc L3 DR Cancel (%) (optional)	Defines the Automatic Congestion Control (ACC) Level 3 (L1) Direct Routed (DR) Cancel Percentage. If a congested condition occurs, the GSX releases this percentage of directrouted calls. A direct routed call is a call that first arrives to a service group for routing, but the GSX has not attempted a retry.
Acc Resp Process (optional)	Sets the Automatic Congestion Control (ACC) Response Process to disabled or enabled. • disabled • enabled When you enable ACC response handling for the service group, and the remote node has indicates a congested (by use of the ACL parameter) state, calls destined to go out the trunk group are set to SKIP (try alternate route) or CANCEL (release the call) depending on the other ACC parameter settings.
Acc Send Acl (optional)	Specifies the maximum ACL value sent to a remote node for this ISUP Service Group. Valid values are between 0 and 3 where 0 disables ACC.

Field	Description
Inspection Time (optional)	Inspection time, specified in datetime format. The INSPECTION parameters provide a method of configuring automatic, regular testing and synchronization of call and maintenance states on all circuits in the ISUP service group. INSPECTION TIME specifies the first datetime at which inspection will occur. Specified in universal octet datetime format. For example, to represent Tuesday May 26, 1992 at 1:30:15 PM EDT, you would specify: 1992526,10:30:15.0,4:0
Inspection Frequency (optional)	Inspection frequency: • onehour • threehours • sixhours • twelvehours • oneday • twodays The default inspection frequency is once per day. The GSX calculates the datetime for each inspection based upon the initial INSPECTION TIME and the frequency. This method maintains the correct frequency and timing even if the GSX has been rebooted.
Inspection State (optional)	Enables or disables circuit inspections
Gateway Outage (optional)	Specifies whether the ISUP service group attempts to keep active calls if the gateway disconnects: Option are: • keepCalls — preserve calls • removeCalls — release calls
OLIP Check (optional)	This setting determines if the GSX performs an Originating Line Information Parameters (OLIP) check on arriving calls with a Charge Number and a Calling Party Number. Options are: on — check for OLIP and reject call if not present off — do not check for OLIP
Info Request Profile	Name of the INR INF profile used by this ISUP service. This name is identical to the name of the ISUP signaling profile used by this ISUP service. This profile specifies the information the system requests if it is not received in the IAM. The GSX provides a default INR INF profile for each ISUP revision.

Field	Description
Satellite Circuits	Specifies whether the circuits in the service group are connected to a satellite: • enabled — circuits are connected to a satellite • disabled — circuits are not connected to a satellite
CLLI Town Code	Specifies the town code used in the CLLI parameter for ANSI GR317 circuit validation test failure. Must be a four character string, default is "0000".
CLLI State Code	Specifies the state code used in the CLLI parameter for ANSI GR317 circuit validation test failure. Must be a two character string, default is "00".
CLLI Building Code	Specifies the building code used in the CLLI parameter for ANSI GR317 circuit validation test failure. Must be a two character string, default is "00".
CLLI Building SubDivision Code	Specifies the building subdivision code used in the CLLI parameter for ANSI GR317 circuit validation test failure. Must be a three character string, default is "000".
Cluster Routing (optional)	Specifies whether this DPC supports cluster routing (also known as member routing). The options are: • supported • unsupported
Sending OLIP Check (optional)	This field turns OLIP checking on or off. When a call with a Charge Number and a Calling Party Number is sent, by default the GSX checks for Originating Line Information Parameters (OLIP) and rejects the call if they are not present. You may wish to disable OLIP checking for certain switches that do not supply OLIP information: • on — check for OLIP • off — do not check for OLIP This check applies only when the GSX, acting as an originating exchange, sends an IAM, the call ingress is nonANSI, and the call egress is ANSI.

Field	Description
Confirmation Tone Name (optional)	Specifies a confirmation tone to play when answering the ISUP call (prior to media cut through). You must configure the confirmation tone as part of the ISUP service group's TONE PACKAGE. Typically, a calling PBX uses a confirmation tone to begin billing.
Alert Tone Name (optional)	The name of a tone type to play on the ingress call when the egress side of the call received an ALERTING message. This may be a ring back tone.
Min Digit for Sending DS Query (optional)	Specifies the minimum number of CalledAddress digits to collect before attempting a route query, when overlap addressing is supported and CalledAddress receive is not complete. The valid range is between 0 and 30 with a default value of 0 (digits).
Confirmation Tone Override (optional)	Specifies support for subscriber level confirmation tone: • supported — a confirmation tone plays for all ingress calls. • unsupported — (default) use the Calling Party Subscriber screen on the PSX to activate the confirmation tone.
Answer Supervision Timeout in Seconds (optional)	If you enable answer supervision, this value specifies the timeout period, in seconds, from the egress receiving the first backwards message from the called party exchange (Call Proceeding, Alerting, Call Progress) until the call is answered. The expiration of the timeout period triggers the answer supervision action specified.
Answer Supervision Timeout Action (optional)	Specifies the action to take if the answer supervision timer expires (that is, no signaled answer is received): • release (default) — release the call. • softanswer — answer the call.
Cut thru Override ACM Received with BCI (optional)	Specifies whether to override the protocol specific cut through direction when the ACM is received with a backward call indicator (BCI) of Interworking Encountered: • unsupported (default) — no override will occur and the protocol specific cut through controls remain in effect. • fullduplexcutthru — perform a full duplex cut through. • nocutthru — perform no cut through
Crankback Profile (optional)	The index number of the Crankback Profile to use with this ISUP service group. You must specify a Call Crankback profile index in the range 1 10. The default is 1.

Field	Description
Sequential GRS (optional)	Specifies whether to issue the Circuit Group Reset Message (GRS) in parallel or sequentially to the circuits. • unsupported — Issue the reset messages in parallel on the circuits. • supported — Reset all circuits by sequentially issuing GRS one at a time per remote point code. This may be necessary for interworking with carriers who become congested or overloaded when processing large numbers of GRS messages at once.

Trunk Group Wizard CIC

This window displays the available CIC ranges for the physical resources selected and allows you to define starting CIC assignments, circuit properties, skip strategies (optional field), starting trunk group member (optional field) and Bellcore CIC assignments for each selected physical resource.

Field	Description
Resources	A list of the physical resources selected in the previous window. To change the selected resources, use the Back button to return to the ISUP Circuits window.
Starting CIC (required)	Defines the starting CIC number for assignment. The system assigns all available channels a CIC number starting with the number entered.
Channels per Span (required)	Defines the number of channels per T1/E1 span
Mode (required)	Defines the mode (blocked or unblocked) of the new circuits
Bellcore	Checking the box indicates the use of the standard Bellcore CIC assignment strategy. Do not use this option if you plan to use a skip channel scenario.
Starting TG Member (optional)	Defines the starting index for assignment of trunk group members. The system assigns trunk group members sequentially starting at the specified index value.
Skip Channel (optional)	Defines a channel index on the resource to skip. If the resource is an E1 or contains E1s, you should use a value of 15; otherwise, leave the field blank. Do not use this option if you plan to use the Bellcore CIC assignment strategy.
Circuit Profile (optional)	Defines the use of a Circuit Service Profile previously configured on the target GSX.

Field	Description
Direction (required)	Indicates which call directions are allowed on this CIC. • Two Way Allows both inbound and outbound • One Way In Allows inbound calls only • One Way Out Allows outbound calls only.

If you need to create additional Service Groups, click the **Another** button to return to the ISUP Service Group window. After creating additional Service Groups, the CIC ranges displayed, will depend upon the Destination Point Code specified. If the DPC is the same as an existing Service Group, the CIC range displayed is for the current Service Group with allowances for CICs allocated to the original Service Group.

Renaming Trunk Groups

You can rename GSX trunk groups on Ribbon Application Management Platform (RAMP). RAMP supports renaming trunk groups on the GSX and the PSX without impacting service.

Unable to render include or excerpt-include. Could not retrieve page.

Prerequisites

- Super User [privileges](#) for **Tools** within the **Core Resources** application.
- A GSX device is registered on RAMP.
- GSX Super User or Provisioner privileges.
- PSX Read/Write privileges for Trunk Group entity.

Start

1. Log on to the [RAMP](#) GUI.
2. Navigate to **Observability > Tools > Trunk Group**.
3. Click the **Renaming** button.
4. Select the GSX from the drop-down list.
5. In the Current Name field, enter the name of the trunk group you wish to rename. The name is case-sensitive and must be exact.
6. Enter the new name for the trunk group in the **New Name** field.
7. Click the **Apply** button. Insight supplies feedback on the process in the **Status** area.

When you use this feature, Insight issues commands that perform the following tasks:

- The system renames the trunk group on the GSX. At this point, the call can be routed to both the old trunk group name and the new trunk group name.
- The system renames the trunk group on the PSX. Since the rename operation takes place on the Primary PSX, the system waits for confirmation from the primary that the information has been replicated to the replica PSXs.
- Upon confirmation of the success of the rename operation on the PSX, the system removes the old trunk group name from the GSX.

If the rename operation succeeds on the GSX, but fails on the PSX, then both trunk group names remain active on the GSX (the old name appears as an Alternate Name under the new named trunk group). Once you resolve the cause of the failure on the PSX you may manually remove the old trunk group name on the GSX using the **Clear Alternate Trunk Group Name** command in the GSX Navigator.

GSX System

Ribbon Application Management Platform (RAMP) allows you to initiate tasks containing one or more GSX commands across all managed GSX devices.

The only supported operation is **Globally Set ISUP Service Message Priority Reset On**, which issues the following CLI commands to each managed GSX devices:

```
SHOW ISUP SERVICE ALL ADMIN
CONFIGURE ISUP SERVICE ALL MESSAGE PRIORITY RESET ON
```

Prerequisites

- Super User [privileges](#) for **Tools** within the **Core Resources** application.
- A GSX device is registered on RAMP.

Start

1. Log onto the RAMP GUI.
2. Navigate to **Observability > Tools > GSX System**.
3. Select a report from the **Reports** drop-down menu. A dialog box displays
4. Select a command from the **Tasks** drop-down menu.
5. Click the **Select** button. A dialog box displays prompting you to confirm.
6. Click **OK**. The task is initiated.

Number Portability Services

In this section:

- [Mobile Number Portability](#)
 - [Deploy MNP Services](#)
 - [Endpoint URLs](#)
 - [Configuring Generic NP Service in RAMP](#)
 - [Configuring the Syniverse MNP Service](#)
 - [Configuring Telcordia MNP Service Information](#)
- [Local Number Portability](#)
 - [Bulk Data Download](#)
 - [View SSH-Keys](#)
 - [Configuring Incremental Client Management](#)
 - [Possible Errors and Troubleshooting](#)

Ribbon Application Management Platform (RAMP) supports the following Number Portability (NP) Services.

- **MNP**: MNP is for Mobile Number Portability in India and other regions. The MNP services are provided by Syniverse Mobile Clearing House (MCH), Telcordia MCH, and Generic Number Portability Clearing House (NPC). The MNP service provides the facility to retain the mobile number when the user switches to another mobile network operator. In India, Donor-led system is used to implement MNP. In this system, the user gets the Porting Authorization Code (PAC) from the current operator and proves the PAC to the new network to continue with the port process.
- **LNP Adaptor**: LNP is for local number portability for US.

Number Portability (NP) services are displayed in the RAMP GUI after deploying LNP and registering a PSX.

Mobile Number Portability

Related articles:

- [Deploy MNP Services](#)
- [Endpoint URLs](#)
- [Configuring Generic NP Service in RAMP](#)
- [Configuring the Syniverse MNP Service](#)
- [Configuring Telcordia MNP Service Information](#)

Ribbon Application Management Platform (RAMP) provides the following synchronization functionality to support Indian Mobile Number Portability (MNP).

Indian MNP service is supported only on Linux platform.

- Bulk Data Synchronization
- Real-time Incremental Synchronization

The above synchronization mechanisms are used to update the hosted MNP data between MCHs database and Local MNP database.

In India, the MCHs are hosted by the following two vendors:

- **Syniverse** – hosts MNP data for northern and western part of India
- **Telcordia** – hosts MNP data for southern and eastern part of India

Generic NP hosts MNP data for any region.

RAMP provides a North Bound Interface (NBI) that implements the SOAP/XML web service interfaces for both the Syniverse and Telcordia MCH to request/receive the bulk/real-time incremental data that contains the MNP data.

When RAMP requests for bulk data synchronization, the MCH creates the bulk files and notifies RAMP. RAMP will process the bulk files and provision the PSX.

The MNP data synchronization must be performed using Bulk Data Synchronization method at the first time. For Bulk Data Synchronization, you need to perform Bulk Data Download (BDD) on RAMP to get the hosted MNP data. The Bulk Data Download is classified into two types as follows:

- **Full Bulk Data Download:** Provides the snapshot of their database as on a particular date. Operators can upload this file onto PSX as part of initial setup.
- **Partial Bulk Data Download:** Provides the list of transactions for a period not exceeding a week. This contains information of ported as well as numbers which returned to their original network.

To enable MNP services, refer to [Deploy MNP Services](#).

To configure the MNP Application Management settings, refer to [MNP Services Parameters](#).

POL-LNP-STORE and RAMP-LNP-FEED-D licenses are required to use this functionality. For more information about these licenses, refer to [Node Locked Licenses on RAMP](#).

If licenses are to be associated/disassociated, MNP services should be restarted.

Deploy MNP Services

The MNP services are deployed with the LNP adaptor. MNP services along with LNP are not deployed by default.

Enable the LNP Adaptor after installing or upgrading the Ribbon Application Management Platform (RAMP).

If the LNP Adaptor is not deployed, the following message appears:

Note

If the configuration fields are set or modified, restart the MNP service.

The Local Number Portability (LNP) Adaptor is not deployed by default on the RAMP.

Start

1. SSH to RAMP as the insight user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the insight user.
2. Stop RAMP:

```
/opt/sonus/ems/emsMgmt stop
```

3. Change to the root user:

```
su - root
```

4. Deploy LNP application:

```
/opt/sonus/ems/conf/deployLNPAApplication.sh
```

5. Change to insight user:

```
sudo su - insight
```

6. Start RAMP:

```
/opt/sonus/ems/emsMgmt start
```

7. For a redundancy RAMP set-up, deploy the LNP Adaptor on RAMP active and standby nodes.

Endpoint URLs

Only the user with admin rights can access Endpoint URLs. If proper credentials are not used, the HTTP 401 error is reported.

- For Syniverse, no user credentials are required for broadcasting.
- For Telcordia, the broadcast credentials will be shared by Telcordia. The **Ribbon Application Management Platform (RAMP)** operator has to configure the given broadcast credentials in the Telcordia MNP page.
- For Generic MNP, the broadcast credentials will be shared by the **RAMP** operator to the Clearing House. Clearing House will pass these credentials.

The following tables provide endpoints information for Syniverse, Telcordia, and Generic NP.

Generic URLs

Endpoint	Information
Service name: {SonusGenericNP.xsd} sonusGeneriNPService	Address:: https://<RAMP IP address>:443/genericNP/ sonusGenericNPService
Port Name: {SonusGenericNP.xsd} sonusGenericNPServicePort	WSDL: https://<RAMP IP address>:443/ genericNP/sonusGenericNPService?wsdl

Syniverse URLs

Endpoint	Information
Service name: {MNPProtocol.xsd}mnp-service	Address:: https://<RAMP IP address>:1688/ syniverseMnp/mnp-service
Port Name: {MNPProtocol.xsd}mnp-servicePort	WSDL: https://<RAMP IP address>:1688/ syniverseMnp/mnp-service?wsdl

Telcordia URLs

Endpoint	Information
Service name: {http://ws.inpac.telcordia.com} NPCWebService	Address:: https://<RAMP IP address>:443/ telcordiaMnp/telcordiamnp-service
Port Name: {http://ws.inpac.telcordia.com} NPCWebServiceHttpSoap12Endpoint	WSDL: https://<RAMP IP address>:443/ telcordiaMnp/telcordiamnp-service?wsdl

Configuring Generic NP Service in RAMP

Generic NP provisioning is not region specific. The Generic NP service consists of the following:

- Full or partial Bulk File upload
- Partial provisioning
- Real-time Number Portability Synchronization

The initial data from the NPC is populated to each of the primary and replica PSX using the PSX BDD tool.

To provision **Ribbon Application Management Platform (RAMP)** Generic NP Service:

1. Configure the primary PSX name if more than one PSX device is registered in RAMP. Refer to [Register a PSX Device](#) for additional details.
2. Configure Generic NP Service Information.
 - a. Log on to RAMP GUI.
 - b. Navigate to **Observability > Tools > NP Services**.
The **NP Services** window displays.
 - c. Expand **Applications**.
 - d. Click **Generic NP**. The **Generic NP Service Information** pane displays.
 - e. Configure Generic NP Service Information.
 - i. Enter the URL in the **NPC Web Service URL :** field.

For example: `http://10.70.52.125:8080/mockService?WSDL`

If the Web Service URL is modified, disable Generic MNP service and enable again.

- ii. Enter the company name in the **Company Name** field.
- iii. Enter the password password in the **Password** field.
- iv. Click **Update**.

The Local Listener Status must no be **NOT LISTENING FOR BROADCAST MESSAGES FROM NPC**.

- f. Upload and provision the Partial Bulk Data file.

Only partial BDD files can be provisioned. However, complete BDD files can also be uploaded.

- i. Click **Browse** and open the bulk file on local system.
- ii. Click **Upload/Provision**.

The status changes to **PROVISIONING**. It is an asynchronous operation, as provisioning takes more time based on the data.

If provisioning is successful, the alarm [sonusEmsNPBulkProvisioningCompletedNotification](#) is raised and the status changes to **PROVISIONED**.

If provisioning fails, the alarm [sonusEmsNPBulkProvisioningFailedNotification](#) is raised and the status changes to **UPLOAD_FAILED**.

- Set the parameter **Receive Messages from Generic NPC** to True, refer to [MNP Services Parameters](#).

Configuring the Syniverse MNP Service

Related articles:

- [Bulk Data File Request for Syniverse MNP](#)

Syniverse MNP hosts MNP data for northern and western part of India.

Follow this procedure to configure Syniverse MNP Service Information on Ribbon Application Management Platform (RAMP):

Note

All the information needed for provisioning will be provided by Syniverse.

- Log on to RAMP GUI.
- Navigate to **Observability > Tools > NP Services**.
- Expand **Applications**.
- Click **Syniverse MNP**.
- Enter the URL in the **MCH Web Service URL** field.

For example: `http://<Syniverse MCH IP>:1689/mnpserver/services/mnp-service`

Note

For Syniverse, the messages from the MNP service needs to be redirected to the port 443. To enable redirection of the messages that arrive at port 1688 to the service at 443, enter the following command on RAMP as a `root` user.

```
iptables -t nat -A PREROUTING --src 0/0 --dst <RAMP IP address> -p tcp --dport 1688 -j REDIRECT --to-ports 443
```

- Provide the ID of the Syniverse MCH that you need to use in the **Syniverse MCH ID** field.
- Provide an appropriate operator ID in the **Operator ID** field.
- Click on **Update**.

Note

The Local Listener Status will be **LISTENING FOR BROADCAST MESSAGES FROM MCH** or **NOT LISTENING FOR BROADCAST MESSAGES FROM MCH**.

Bulk Data File Request for Syniverse MNP

Perform the following procedure on Ribbon Application Management Platform (RAMP) to request the bulk data file from MCH:

1. Log on to RAMP GUI.
2. Navigate to **Observability > Tools > NP Services**.
3. Expand **Applications**.
4. Click **Syniverse MNP**.
5. Select the required database type from the **Database Type** option.

Database types include Full or Partial. If the option selected is partial, mention the dates under **Date range** option. Ensure the Date range is not more than a week.

6. Click **Request Bulk File**.

On clicking **Request Bulk File**, the "Last Download Request Status" table is added with a new request **"WAITING_MCH_RESPONSE"**. Once the MCH generates the bulk file, it sends a bulk file response to RAMP. RAMP then raises a trap [sonusEmsNPBulkFileReadyNotification](#) and the status changes to **MCH_RESPONSE_RECEIVED**.

If there is an error in the request, MCH rejects the request and sends an error response. In this case, RAMP raises a trap [sonusEmsNPBulkFileRequestRejectedNotification](#). On refreshing the page the status of the request changes to **MCH_ERROR**.

Views the summary of the error from the "Detail" window of the Bulk File Request or from the "Trap Summary" of the Fault Manager.

7. Refresh the Syniverse MNP page to view the file location. The **Last Download Request Status** screen appears as shown below.

Syniverse Last Download Request Status

Last Download Request Status						
☐	Transaction ID	Type	Sent Time	Status	Received Time	File Location
☐	808-201404090459540000	FULL	2014-04-09 04:59:54.0	MCH_RESPONSE_RECEIVED	2014-04-09 05:02:03.0	DL401
☐	808-201404090500010000	PARTIAL	2014-04-09 05:00:01.0	MCH_RESPONSE_RECEIVED	2014-04-09 05:02:56.0	DL442

Bulk Data File Path:

8. The Bulk files are generated and stored in the location mentioned under **File Location** field.
9. Download the bulk files manually from MCH portal to the local system. MCH portal link and credentials will be shared by Syniverse.

MCH generates 11 *.gz files for a single bulk file request. Hence, gzip compressed tar archive (.tar.gz) of the 11 *.gz files have to be created and the .tar.gz file needs to be uploaded to RAMP.

10. Browse the downloaded bulk file on local system.
11. Upload to RAMP using **Upload/Provision** Button. The **Last Download Request Status** with the status as **Uploaded** is as shown below:

Syniverse Last Download Request Status-Uploaded

Last Download Request Status						
☐	Transaction ID	Type	Sent Time	Status	Received Time	File Location
☒	808-201404090459540000	FULL	2014-04-09 04:59:54.0	UPLOADED	2014-04-09 05:02:03.0	DL401
☐	808-201404090500010000	PARTIAL	2014-04-09 05:00:01.0	MCH_RESPONSE_RECEIVED	2014-04-09 05:02:56.0	DL442

Bulk Data File Path:

Full BDD file shall only be uploaded to RAMP. For provisioning the full BDD file to PSX, refer to [PSX Provisioning](#) documentation. After uploading, the status changes to either UPLOADED or UPLOAD_FAILED. It is a synchronous operation.

In case of Partial BDD, the status changes to **PROVISIONING**. It is an asynchronous operation, since provisioning takes more time based on the data. RAMP raises either of the two traps ([sonusEmsNPBulkProvisioningCompletedNotification](#) and [sonusEmsNPBulkProvisioningFailedNotification](#)). On refreshing the page, the status changes to either **PROVISIONED** or **PROVISIONING_FAILED**.

Configuring Telcordia MNP Service Information

Related articles:

- [Bulk Data File Request](#)

Telcordia MNP hosts MNP data for southern and eastern part of India.

Follow this procedure to configure the Telcordia MNP Service Information on Ribbon Application Management Platform (RAMP).

All the information needed for provisioning will be provided by Telcordia.

1. Log on to RAMP GUI.
2. Navigate to **Observability > Tools > NP Services**.
3. Expand **Applications**.
4. Click **Telcordia MNP**.
5. Provide the URL in the **MCH Web Service URL** field.
For example: `https://<Telcordia MCH IP>/NPCWebApp/services/NPCWebService`
6. Provide the participant ID in the **Participant ID** field.
7. Under **MCH Service Credentials**, provide the user name and password in the **User Name** and **Password** fields.
8. Under **Broadcast Validation Credentials**, provide the user name and password in the **User Name** and **Password** fields.
9. Click on **Update**.

The Local Listener Status will be **NOT LISTENING FOR BROADCAST MESSAGES FROM MCH** or **LISTENING FOR BROADCAST MESSAGES FROM MCH**.

Bulk Data File Request

Perform the following procedure on Ribbon Application Management Platform (RAMP) to request the bulk data file from MCH.

1. Log on to RAMP GUI.
2. Navigate to **Observability > Tools > NP Services**.
3. Expand **Applications**.
4. Click **Telcordia MNP**.
5. Select the required database type from the **Database Type** option.
6. Click **Request Bulk File**.

On clicking **Request Bulk File**, the “Last Download Request Status” table is added with a new request “**WAITING_MCH_RESPONSE**”. Once the MCH generates the bulk file, it sends a bulk file response to RAMP. RAMP then raises a trap “sonusEmsNPBulkFileReadyNotification” and the status changes to **MCH_RESPONSE_RECEIVED**.

If there is an error in the request, MCH rejects the request and sends an error response. In this case, RAMP raises a trap “sonusEmsNPBulkFileRequestRejectedNotification”. On refreshing the page the status of the request changes to **MCH_ERROR**. The summary of the error can be viewed in Detail window of the Bulk File Request or in Trap Summary in Fault Manager.

7. Refresh the Telcordia MNP page to view the file location. The **Last Download Request Status** screen appears as shown below.

Last Download Request Status

☐	Transaction ID	Type	Sent Time	Status	Received Time	File Location
☐	AP201404090505278080009	FULL	2014-04-09 05:05:27.0	MCH_RESPONSE_RECEIVED	2014-04-09 05:02:03.0	/ftp/AP808/NPCDownloadF_AP20140408_180950.xml
☐	AP201404090525108080020	PARTIAL	2014-04-09 05:25:10.0	MCH_RESPONSE_RECEIVED	2014-04-09 05:02:03.0	/ftp/AP808/NPCDownloadD_AP20140408_1809.xml
☐	AS201404090505278080006	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	AS201404090525108080017	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	BR201404090505278080002	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	BR201404090525108080013	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	KA201404090505278080000	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	KA201404090525108080011	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	KL201404090505278080004	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	KL201404090525108080015	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	KO201404090505278080003	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	KO201404090525108080014	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	MP201404090505278080005	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	MP201404090525108080016	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	NE201404090505278080007	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	NE201404090525108080018	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	OR201404090505278080010	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	OR201404090525108080021	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	TN201404090505278080001	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	TN201404090525108080012	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	WB201404090505278080008	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	WB201404090525108080019	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		

Bulk Data File Path:

- The Bulk files are generated and stored in the location mentioned under **File Location** field.
- Download the bulk files manually from MCH portal.

MCH generates the bulk files in the xml format for Telcordia MNP service

- Browse the downloaded bulk file on the local system.
- Upload to RAMP using **Upload/Provision** button. The **Last Download Request Status** with the status as **Uploaded** is as shown below.

Last Download Request Status

☐	Transaction ID	Type	Sent Time	Status	Received Time	File Location
☐	AP201404090505278080009	FULL	2014-04-09 05:05:27.0	UPLOADED	2014-04-09 05:02:03.0	/ftp/AP808/NPCDownloadF_AP20140408_180950.xml
☐	AP201404090525108080020	PARTIAL	2014-04-09 05:25:10.0	MCH_RESPONSE_RECEIVED	2014-04-09 05:02:03.0	/ftp/AP808/NPCDownloadD_AP20140408_1809.xml
☐	AS201404090505278080006	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	AS201404090525108080017	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	BR201404090505278080002	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	BR201404090525108080013	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	KA201404090505278080000	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	KA201404090525108080011	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	KL201404090505278080004	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	KL201404090525108080015	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	KO201404090505278080003	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	KO201404090525108080014	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	MP201404090505278080005	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	MP201404090525108080016	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	NE201404090505278080007	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	NE201404090525108080018	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	OR201404090505278080010	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	OR201404090525108080021	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	TN201404090505278080001	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	TN201404090525108080012	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		
☐	WB201404090505278080008	FULL	2014-04-09 05:05:27.0	WAITING_MCH_RESPONSE		
☐	WB201404090525108080019	PARTIAL	2014-04-09 05:25:10.0	WAITING_MCH_RESPONSE		

Bulk Data File Path:

Full BDD file shall only be uploaded to RAMP. For provisioning the full BDD file to PSX, refer to [PSX Provisioning](#) documentation. After uploading, the status changes to either `UPLOADED` or `UPLOAD_FAILED`. It is a synchronous operation.

In case of Partial BDD, the status changes to **PROVISIONING**. It is an asynchronous operation, since provisioning takes more time based on the data. RAMP raises either of the two traps (`sonusEmsNPBulkProvisioningCompletedNotification`, `sonusEmsNPBulkProvisioningFailedNotification`). On refreshing the page, the status changes to either **PROVISIONED** or **"PROVISIONING_FAILED"**.

Local Number Portability

Related articles:

- [Bulk Data Download](#)
- [View SSH-Keys](#)
- [Configuring Incremental Client Management](#)
- [Possible Errors and Troubleshooting](#)

The Local Number Portability (LNP) Adaptor synchronizes and sends LNP data received from the National Portability Administration Center (NPAC) at multiple locations simultaneously. NPAC, the national database, contains the routing information for all ported and pooled numbers in the US and Canada. NPAC supports Local Number Portability (LNP) across service providers.

The PSX is the repository for the LNP data received from NPAC. [Ribbon Application Management Platform \(RAMP\)](#) receives the LNP data from NPAC via the SIP-IX interface. RAMP parses and provisions the LNP data into the PSX Primary using the PIPE interface. The PSX-Replica stores this data in its database. Refer to [Hosted LNP Service](#).

Ribbon supports incremental LNP updates over SOAP from NPAC and offline bulk data download (BDD) files. You can add multiple NPAC servers on RAMP to support BDD and Incremental Synchronizer Management.

RAMP receives the first LNP data snapshot in the form of an initial BDD file. An administrator can download the BDD file from RAMP. The BDD file is available on RAMP until the operator deletes it.

The BDD files are stored on RAMP at `opt/sonus/ems/weblogic/sonusEms/data/lnp/`. The file is carried forward during release upgrades.

You can add and delete NPAC servers on RAMP and download and synchronize LNP data from all the servers.

The LNP Adaptor object tree contains the following node objects:

- Bulk Data Download
- Incremental Client Management

POL-LNP-STORE and RAMP-LNP-FEED licenses are required to use this functionality. For more information about these licenses, refer to [Node Locked Licenses on RAMP](#).

Bulk Data Download

Bulk data download is covered in this section.

Prerequisites

For Ribbon Application Management Platform (RAMP) on cloud, perform the FTP on the PSX as the insight user. To log on to the RAMP as the insight user, change the insight password. Refer to [Change Linux Insight User Password on RAMP Standalone](#).

Start

To download BDD file from the external FTP server:

1. Log on to the [RAMP GUI](#).
2. Navigate to **Observability > Tools > NP Services**.
The **NP Services** window displays.
3. From the **Applications** object tree, select **Bulk Data Download**. The **LNP Adaptor - Bulk Data File FTP Download** pane displays.
4. Click the **Add NPAC** button. The **Add NPAC** pane displays.
5. In the **Bulk Data File Path** field, enter the bulk data file path.
6. In the **FTP Server IP Address** field, enter the FTP server IP Address to download the bulk data file.
7. In the **FTP Server User Name** field, enter the FTP server user name.
8. Perform one of the following:
 - To use SSH-Key authentication, select the **SSH-Key** tab. Refer to [View SSH-Keys](#).
 - To use Password authentication:
 - i. Select the **Password** tab.
 - ii. In the **FTP Server Password** field, enter the FTP server password.
9. Click **Download**. The BDD files are downloaded.

After successful BDD file download, the Download Status displays as COMPLETED and the Last Transaction ID is displayed. For more information, refer to [BDD parameters](#).

Note

The BDD files occupy additional disk space which can slow down RAMP. Before initiating BDD, delete the files in the following folders:

- `/opt/sonus/ems/weblogic/sonusEms/data/lnp/tmp/<NPAC ID>`
- `/opt/sonus/ems/weblogic/sonusEms/data/lnp/final/<NPAC ID>`

The NPAC ID is created automatically when BDD is initiated through the RAMP GUI.

The files required by the PSX are located in the directory `/opt/sonus/ems/weblogic/sonusEms/data/lnp/final/<NPAC ID>`.

Save these files in another location for future use.

BDD Parameters

Field	Definition
Bulk Data File Path	The bulk data file path to download the BDD file.
FTP Server IP Address	The FTP server IP address to download the bulk data file.
FTP Server User Name	The FTP server user name.
FTP Server Password	The FTP server password.
Authentication Type	The FTP authentication method. Select one of the following: • SSH-Key: To use SSH-Key authentication. • Password: To use Password authentication.
FTP Server Password	The parameter is applicable only if the Authentication Type is set as password.
Last Download Request Status	The download status and the last transaction ID. After a successful BDD file download, the last transaction ID displays. This ID is generated only if the status is COMPLETE. Status messages during download: • NOT STARTED: Download is yet to start. • IN PROGRESS: Download operation is still in process. • DOWNLOAD ERROR: Error during download. • PARSE ERROR: Package download is completed, but there is an error while obtaining the last transaction ID. For obtaining the last transaction ID, refer to PARSE_ERROR. • COMPLETED: BDD files are downloaded and the last transaction ID is obtained. • FILE_NOT_FOUND: File is not available on the FTP server.

View SSH-Keys

Share the SSH keys and Ribbon Application Management Platform (RAMP) IP address with the NPAC third-party administrator before downloading the LNP file. For (RAMP redundancy, share the IP addresses and SSH keys of the active and standby nodes.

To view SSH keys:

1. Log on to the RAMP GUI.
2. Navigate to **Monitoring > Tools > NP Services**. The **NP Services** pane displays.
3. From the **Applications** object tree, select **Bulk Data Download**. The **LNP Adaptor - Bulk Data File FTP Download** pane displays.
4. Click the **SSH Keys** button. The SSH Keys dialog box displays.
5. Click the **Copy** button to copy the SSH keys.

Configuring Incremental Client Management

The Ribbon Application Management Platform (RAMP) receives periodic updates from NPAC. Configure Incremental Client Management for periodic download.

To configure Incremental Client Management for periodic download of the LNP data:

Note

The incremental feed can be enabled only after the LNP BDD data has been loaded to all the PSX devices. Refer to [Hosted LNP Service](#).

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Tools > NP Services**. The **NP Services** pane displays.
3. From the **Applications** object tree, select **Incremental Synchronizer Management**. The **LNP Adaptor - Incremental Synchronizer Management** pane appears.
4. In the **Web Services URL** field, enter the URL to access the Web Service.
5. In the **Context** field, enter the context to access the NPAC server.
6. In the **Synchronization Interval** drop-down menu, select an interval.
7. In the **Last Synchronized Transaction ID** field, enter the transaction ID.
8. Click **Start**.

The NPAC servers are synchronized with RAMP to periodically download LNP data from for the NPAC servers.

Note

Click **Reschedule** to reschedule the incremental synchronizer.

Click **Stop** to terminate the process.

NPAC parameters for Incremental Synchronizer Management

Field	Description
Web Services URL	The URL to access the Web Service.
Context	The context to access the NPAC server. This parameter is used for authorization of incremental synchronization requests from RAMP. Enter the value "ribbon".
Synchronization Interval	The interval for synchronizing the LNP data interval.
Manually override Transaction Id	The BDD is initiated from the PSX. Manually override and enter the ID when a BDD is initiated on the PSX using BDD Command Center Tool and incremental synchronizer is run on RAMP. The ID is obtained from the BDD file name. The transaction ID is the last value in a BDD file name. For example: In <i>ne.sv_BDD_PSTN_17-02-2015092157.21846810.bdd</i>, the transaction id is <i>21846810</i>. For more information on how BDD is initiated from the PSX, refer to Starting the BDD Command Center Tool and BDD Command Center Tool Menu Options.

Field	Description
Last Synchronized Transaction ID	The last transaction ID is obtained from the BDD file or from the last periodic synchronization interval based on how the BDD is initiated. BDD is initiated from RAMP. Obtain the last transaction ID from Last Download Request Status window, refer to Bulk Data Download. Note Last Transaction ID is visible only if Last Download Request Status is displayed as Complete.
Synchronization Status	Displays the synchronization status. It displays the Client Status, Last Synchronized Transaction Identifier, and Last Successful Synchronization Time.
Locked by Insight	Releases the synchronization if locked by RAMP.

Possible Errors and Troubleshooting

The following section provides information on possible errors on Ribbon Application Management Platform (RAMP) and actions that you can take to rectify the situation.

PARSE_ERROR

- The package download is complete, but there is an error while obtaining the last transaction ID.

To obtain the last transaction ID, perform the following procedure:

- SSH to RAMP.
- Navigate o the directory to `/opt/sonus/ems /weblogic/sonusEms/data/lmp/tmp/`.
- Extract the tar containing BDD files.
- Move `*SV*BDD` and `*BLOCK*BDD` files to `/opt/sonus/ems/weblogic/sonusEms/data/lmp/final/`.

These BDD file names contain last transaction ID.

The BDD file names for LNP data use the following format:

```
<Region>.<BDD_type>_BDD_PSTN_<DD-MM-YYYYHHMMSS>.<TRANS_ID>
```

For example:

```
mw.lrn_BDD_PSTN_26-05-2009212322.1000074.bdd
```

The last transaction ID in the example is 1000074 and it is used for starting incremental changes.

- Use this transaction ID to start incremental changes by overriding last transaction ID.

Joint Interoperability Test Command

In this section:

- [Workflow to Deploy JITC on RAMP](#)
- [Update the Configuration File for JITC](#)
- [Configure RAMP GUI to Comply with JITC](#)
- [Configure RAMP for TLS Communication](#)
- [Configure NTP Server Authentication](#)

The Ribbon Application Management Platform (RAMP) supports Joint Interoperability Test Command (JITC) / Federal Information Processing Standard (FIPS) and Security Technical Implementation Guidelines (STIGs). JITC is the Department of Defence's joint interoperability compliance test agency for information technology.

For RAMP to support JITC/FIPS, enable the FIPS and STIG parameters when you install RAMP. Perform the steps outlined in the [Workflow to Deploy JITC on RAMP](#) to enable and configure RAMP for JITC/FIPS.

Note

- To disable JITC/FIPS in RAMP, re-install RAMP again, without enabling the FIPS/JITC parameters.
- If JITC/FIPS is disabled in RAMP, all registered devices are supported.
- Migration from EMS to FIPS/ JITC-enabled RAMP is not supported.
- To upgrade, perform the regular delete/ create procedures and enable the JITC/ FIPS during the installation.

Note

RAMP with JITC/FIPS enabled does not facilitate direct upgrades.

- RAMP CNF does not support JITC/FIPS.

Workflow to Deploy JITC on RAMP

Perform the following steps to enable, configure, and use Joint Interoperability Test Command (JITC) / Federal Information Processing Standard (FIPS) and Security Technical Implementation Guidelines (STIGs) on the Ribbon Application Management Platform (RAMP).

Start

Step	Action
1	Manually install RAMP based on your deployment model: • Installing RAMP on VMware Manually. • Installing RAMP on KVM Manually. Note When you are updating the configuration file, refer to Update the Configuration File for JITC.

Step	Action
2	Configure RAMP GUI to Comply with JITC.
3	Configure RAMP for TLS Communication.
4	Enable the remote syslog server. For more information, refer to Exporting Logs to a Remote Syslog Server .
5	Change the default passwords.
6	Update the certificates.
7	Configure local and external authentication of admin users. Note • The minimum password length for a JITC/FIPS enabled RAMP is 15 alphanumeric characters. • Enable the Password Aging threshold parameter field and set it to 60 days.
8	For local accounts, enable Force Password Change on initial login. For more information, refer to Add Users .
9	Set the User Timeout Session to 10 minutes using Set Session Expiry in RAMP GUI .

Step	Action
10	Disable SOAP API settings. 1. Disable to PSX SOAP API Settings: Note Set anything with Deploy PSX version X.X.X as False. This is to ensure that none of the PSX SOAP APIs are deployed. For more information, refer to Application Configuration EMS API Parameters. 2. Disable SGX SOAP API Settings Note ◦ Set Deploy version 5.2.1 to False. ◦ Disable SGX SOAP API settings. For more information, refer to Application Configuration SGX API Parameters.
11	Set the disk usage threshold to 75%. For more information, refer to Create a Threshold. Use the following values: • Node Type: RAMP • Category: InsightFsUsageStats • Name: USAGE • Trigger value: 75 • Clearing value: 65 • Severity: MAJOR • Notify on clearing threshold crossed: ON • Enabled: ON Note When the file system usage crosses 75% an alarm is raised. It is automatically cleared when the usage drops to 65% and less.
12	Take a Backup of RAMP.
13	Network Time Protocol (NTP) server authentication: Add NTP Servers. NTP server authentication: Configure NTP Server Authentication.

Step	Action
14	For RAMP to support JITC/FIPS, enable SNMPv3 on the PSX and SBC devices. Refer to Register a PSX Device and Register an SBC Core Device. Use the following values to update the SNMPv3 settings: • SNMPv3 Security Level: AuthNoPriv • SNMPv3 User: <username> • SNMPv3 Authentication Protocol: SHA • SNMPv3 Auth Passphrase: <passphrase> • SNMPv3 Privacy Protocol: AES • SNMPv3 Privacy Passphrase: <passphrase> Note AES128 and SHA are used.
15	To temporarily disable remote access, refer to How to Start and Stop RAMP .

Update the Configuration File for JITC

Update the configuration file to deploy an instance of the Ribbon Application Management Platform (RAMP) on the Kernel Virtual Machine (KVM) for Joint Interoperability Test Command (JITC). RAMP uses the values in this file during installation.

Start

1. Log on to the KVM host as a `root` user.
2. Navigate to the directory in which the `qcow2` and `configDriveImgDeployment.img` files are downloaded.
3. Create a temporary mount directory:

Example

```
mkdir -p /tmp/vmconf
```

4. Mount the `configDriveImgDeployment.img` file in the temporary mount directory:

```
mount -o loop configDriveImgDeployment.img /tmp/vmconf
```

Note

Use a different mount directory to create multiple instances of KVM and create a `configDriveImgDeployment.img` file for each instance.

5. Modify the `configDriveImgDeployment.img` file for your deployment using the values in the following table:

```
vim /tmp/vmconf/user-data
```

user-data Parameters

Key Name	Description	Mandatory (M)/Optional (O)	Example Value
timezone	Specifies the time zone for your network in which the VM is created.	M	Asia/Kolkata
ntpServer	Specifies the NTP server IP address, if applicable. To add multiple NTP servers (up to 5 are allowed), enter the NTP server IP addresses in the following format: servers: ◦ \$ntpServer1 ◦ \$ntpServer2 ◦ \$ntpServer3 ◦ \$ntpServer4 ◦ \$ntpServer5	M	servers: ◦ 10.128.254.67 ◦ 10.128.254.68 ◦ 10.10.211.119
dnsServer	Specifies the IP address of the DNS server.	O	IPV4: 10.128.254.67 IPV6: 0:0:0:0:ffff:c0a8:101
dnsSearchPath	Search path for the DNS server.	O	rbbn.com
InstanceName	Specifies the RAMP instance or virtual machine (VM) name. The <code>InstanceName</code> criteria: ◦ Uppercase or lowercase letters [a-z], [A-Z]. ◦ Digits [0-9]. ◦ Do not begin the name with a digit. ◦ Do not use special characters, including the hyphen.	M	rampSA

Key Name	Description	Mandatory (M)/Optional (O)	Example Value
EnableFips	Enter Y to enable FIPS while installing RAMP for JITC. The options are: ◦ Y: enable FIPS. ◦ N: disable FIPS. By default FIPS is disabled.	M	N/A
EnableStig	Enter Y to enable STIG while installing RAMP for JITC. The options are: ◦ Y: enable STIG. ◦ N: disable STIG. By default STIG is disabled.	M	N/A

Key Name	Description	Mandatory (M)/Optional (O)	Example Value														
stigIDs	The variable specifying the application impacting STIGs: Update the following STIG IDs in the configuration drive based on your requirements:	M	N/A														
	<table><tr><th>STIG-ID</th><th>Description</th></tr><tr><td>V230313</td><td>RHEL 8 must disable core dumps for all users.</td></tr><tr><td>V230496</td><td>RHEL 8 must disable the stream control transmission protocol (SCTP).</td></tr><tr><td>V230384</td><td>RHEL 8 must set the unmask value to 077 for all local interactive user accounts</td></tr><tr><td>V230344</td><td>RHEL 8 must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.</td></tr><tr><td>V237643</td><td>RHEL 8 must require re-authentication when using the "sudo" command.</td></tr><tr><td>V230489</td><td>RHEL 8 must not have the <code>sendmail</code> package installed.</td></tr></table>			STIG-ID	Description	V230313	RHEL 8 must disable core dumps for all users.	V230496	RHEL 8 must disable the stream control transmission protocol (SCTP).	V230384	RHEL 8 must set the unmask value to 077 for all local interactive user accounts	V230344	RHEL 8 must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.	V237643	RHEL 8 must require re-authentication when using the "sudo" command.	V230489	RHEL 8 must not have the <code>sendmail</code> package installed.
	STIG-ID			Description													
	V230313			RHEL 8 must disable core dumps for all users.													
	V230496			RHEL 8 must disable the stream control transmission protocol (SCTP).													
	V230384			RHEL 8 must set the unmask value to 077 for all local interactive user accounts													
	V230344			RHEL 8 must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period.													
	V237643			RHEL 8 must require re-authentication when using the "sudo" command.													
V230489	RHEL 8 must not have the <code>sendmail</code> package installed.																

Key Name	Description		Mandatory (M)/Optional (O)	Example Value			
	<table><tr><th>STIG-ID</th><th>Description</th></tr><tr><td>V244545</td><td>RHEL 8 must enable Fapolicy module configurations to employ a deny-all, permit-by-exception policy to allow the running of authorized software programs.</td></tr></table>	STIG-ID	Description	V244545	RHEL 8 must enable Fapolicy module configurations to employ a deny-all, permit-by-exception policy to allow the running of authorized software programs.		
STIG-ID	Description						
V244545	RHEL 8 must enable Fapolicy module configurations to employ a deny-all, permit-by-exception policy to allow the running of authorized software programs.						
IF1							
GWV4	NOTE: This parameter is applicable only if you are creating a RAMP VM in an IPv4 network. The gateway IP address from the available network pool in IPv4. "1" indicates the interface number.	M	192.168.1.1				
IPV4	NOTE: This parameter is applicable only if you are creating a RAMP VM in an IPv4 network. The fixed management IPv4 address for the interface. ◦ IF1Ipaddr is the IP address of eth0 ◦ IF2Ipaddr is the IP address of eth1	M	192.168.1.7/24				
GWV6	NOTE: This parameter is Mandatory if RAMP is configured as IPV6. The gateway IP address from the available network pool in IPV6. "101" indicates the interface number	O/M	0:0:0:0:ffff:c0a8:101				

Key Name	Description	Mandatory (M)/Optional (O)	Example Value
IPV6	NOTE: This parameter is Mandatory if RAMP is configured as IPV6. The fixed management IPv6 address for the interface and netmask. ◦ IF1paddrv6 is the IP address of eth0 ◦ IF2lpaddrv6 is the IP address of eth1	O/M	0:0:0:0:ffff:c0a8:107/64
Port	The network port number for the interface. The interface numbering is in the following pattern: ◦ eth0 ◦ eth1 ◦ eth2	M	eth0

Example of an Input File

```
#cloud-config
timezone: "Asia/Kolkata"
ntp:
  enabled: true
  ntp_client: chrony
  config:
    conffpath: /etc/chrony.conf
    check_exe: chronyd
    packages:
      - chrony
    service_name: chronyd
    template: |
      ## template:jinja
      # My NTP Client config
      {%- if servers %}# servers
      {% endif %}
      {% for server in servers -%}
      server {{server}} iburst
      {% endfor %}
  servers:
    - 10.xx.xx.xx
    - $ntpServer2
    - $ntpServer3
    - $ntpServer4
    - $ntpServer5
```

```

manage_resolv_conf: true
resolv_conf:
  nameservers: ['$dnsServer']
  searchdomains:
    - $dnsSearchPath
write_files:
  - path: /opt/rbbn/userData.json
    permissions: '0644'
    content: |
      {
        "IF1": {"GWV4": "10.xx.xx.1", "IPV4": "10.xx.xx.xx/24", "Port": "eth0"},
        "IF2": {"GWV4": "", "IPV4": "/", "Port": ""},
        "growpart": { "opt" : 60, "pgsql": 30, "home": 10},
        "InstanceName": "rampinstance1",
        "EnableFips": "Y",
        "EnableStig": "Y",
        "stigIDs" : ["V230313", "V230344", "V237643", "V230489", "V230496", "V230384", "V244545"]
      }
    owner: root:root
  runcmd:
    - usermod -p '$1$admin$1kgWpnZpUx.vTroWPXPIB0' admin

```

You can enable just FIPS alone without STIGs by adding "EnableFips" = "Y" entry alone in the user-data file

6. Save and close the configuration file.
7. Unmount the image:

```
umount /tmp/vmconf
```

8. Delete the temporary mount point:

```
rm -rf /tmp/vmconf
```

9. Return to the workflow on [Installing RAMP on KVM Manually](#).

Configure RAMP GUI to Comply with JITC

In this section:

- [Create an Interface for Client Certificate](#)
- [Create and Sign the Certificate Authority, Server Certificate, and Client Certificate](#)
- [Customize the Logon Banner](#)
- [Install Certificates on RAMP and the Browser](#)
- [Log on to JITC Enabled RAMP](#)

Related topics:

- [Joint Interoperability Test Command](#)
- [Workflow to Deploy JITC on RAMP](#)
- [Update the Configuration File for JITC](#)
- [Manually Enable or Disable FIPS/JITC and STIG](#)

Perform the following procedures to configure the Ribbon Application Management Platform (RAMP) to comply with the Joint Interoperability Test Command (JITC) / Federal Information Processing Standard (FIPS):

Create an Interface for Client Certificate

Prerequisites

For the list of user and roles administration, refer to [Authentication and Authorization information on User Privileges in RAMP](#).

Start

1. Log on to the RAMP GUI using `admin/admin` as the username and password.
2. Navigate to **Management > Authentication & Authorization > Users**. The **Users** window displays.
3. Click **+ Add User** to create a new user. For more information on creating a new user, refer to [Add Users](#).

Note

Ensure the created user name and the name of the client certificate are identical.

Create and Sign the Certificate Authority, Server Certificate, and Client Certificate

Use the following procedure to create certificates on RAMP:

Note

Replace all occurrences of `"ramp-client-cert-user-name"` with your RAMP client certificate user name and `"emailAddress"` with your email address.

1. Log on as a `root` user.
2. Create a common directory for all the certificates:

```
sudo su -
cd /etc/httpd/conf
mkdir jitc
cd jitc
```

3. Generate the Certificate Authority (CA) for `cakey.pem` and `cacert.pem`:

```
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -pkeyopt
rsa_keygen_pubexp:65537 -out cakey.pem
openssl req -new -x509 -key cakey.pem -out cacert.pem -days 1095 -subj '/C=US/
ST=MA/L=Westford/O=Ribbon/OU=Ribbon CA/CN=ramp-client-cert-user-name/
emailAddress=admin@rbbn.com'
```

4. Generate the server key and request:

```
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -pkeyopt
rsa_keygen_pubexp:65537 -out rampKey.pem
openssl req -new -key rampKey.pem -out rampreq.csr -subj '/C=US/ST=MA/L=Westford/
O=.Ribbon/OU=.Ribbon CA/CN=ramp-client-cert-user-name/emailAddress=admin@rbbn.com'
```

5. Sign the server certificate:

```
cp cakey.pem /etc/pki/CA/private/
cp cacert.pem /etc/pki/CA/
touch /etc/pki/CA/index.txt
echo 02 > /etc/pki/CA/serial
openssl ca -in rampreq.csr -out rampcert.pem
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
```

Note

If the error message "ERROR:Serial number 02 has already been issued,..." displays after repeating this step, resolve the error by ensuring that the `/etc/pki/tls/openssl.conf` file includes the following configuration:

```
dir = /etc/pki/CA # TSA root directory
Change the attribute in /etc/pki/CA/index.txt.attr: "unique_subject =
no"
Or empty /etc/pki/CA/index.txt
```

6. Verify the Server Certificate:

```
cp cacert.pem cert-ourca.crt
openssl verify -CAfile cert-ourca.crt rampcert.pem
```

A Sample Output

```
rampcert.pem: OK
```

7. Generate the client certificate:

```
cd /etc/httpd/conf/jitc
openssl genrsa -out clientuser.key 2048
openssl req -new -key clientuser.key -out clientuser.csr -subj '/C=US/ST=MA/
L=Westford/O=.Ribbon/OU=.Ribbon CA/CN=ramp-user-name/emailAddress=admin@rbbn.com'
openssl ca -in clientuser.csr -out clientuser.pem
```

8. Verify the client certificate and generate `clientuser.p12` :


```
cp clientuser.pem clientuser.crt
openssl verify -CAfile cert-ourca.crt clientuser.pem
openssl pkcs12 -export -in clientuser.crt -CAfile cert-ourca.crt -inkey
clientuser.key -out clientuser.p12
"Enter" twice to leave password blank (2nd time won't have this step)
"Enter" twice to leave password blank
```

9. Update the Apache configuration with the CA and `servercert` path.

a. Log on as an `insight` user.

- i. Edit the `/opt/sonus/ems/weblogic/sonusEms/data/sys/emsapps_apacheproxy_virtual_host.conf` file and comment out the current path as following:

```
##### Mutual TLS Support: comment start
#####
    SSLCertificateFile    /etc/httpd/conf/InsightCert.cert
    SSLCertificateKeyFile /etc/httpd/conf/InsightCertKey.pem
##### Mutual TLS Support: comment end
#####
```

- ii. Un-comment and update the paths as following:

```
##### uncomment and update start
#####
# SSLVerifyClient optional
# SSLVerifyDepth 10
# SSLCertificateFile "/etc/httpd/conf/jitc/rampcert.pem"
# SSLCertificateKeyFile "/etc/httpd/conf/jitc/rampKey.pem"
# SSLCACertificateFile "/etc/httpd/conf/jitc/cert-ourca.crt"
##### uncomment and update end
#####
```

b. Log on as a `root` user.

- i. Run the following commands:

```
# cp /etc/httpd/conf/jitc/cert-ourca.crt /home/admin/
# chown insight:insight /home/admin/cert-ourca.crt
# chmod 775 /home/admin/cert-ourca.crt
```

c. Log on as `insight` user.

- i. Run the following commands:

```
cp -p /opt/rbbn/pm/conf/secure/pm-ms.truststore /opt/rbbn/pm/conf/secure/pm-
ms.truststore.original
```

```
keytool -importcert -file /home/admin/cert-ourca.crt -alias <alias>
-keystore /opt/rbbn/pm/conf/secure/pm-ms.truststore -storetype BCFKS
-storepass ribbonpm

cp -p /opt/rbbn/lm/config/secure/lm-ms.truststore /opt/rbbn/lm/config/secure/
lm-ms.truststore.original
keytool -importcert -file /home/admin/cert-ourca.crt -alias <alias>
-keystore /opt/rbbn/lm/config/secure/lm-ms.truststore -storetype BCFKS
-storepass ribbonlm

cp -p /opt/devMgmt/conf/secure/devmgmt-ms.truststore /opt/devMgmt/conf/
secure/devmgmt-ms.truststore.original
keytool -importcert -file /home/admin/cert-ourca.crt -alias <cert name>
-keystore /opt/devMgmt/conf/secure/devmgmt-ms.truststore -storetype BCFKS
-storepass ribbonpm

cp -p /opt/sonus/ems/weblogic/sonusEms/data/sys/ems.keystore /opt/sonus/ems/
weblogic/sonusEms/data/sys/ems.keystore.original
keytool -importcert -file /home/admin/cert-ourca.crt -alias <cert name>
-keystore /opt/sonus/ems/weblogic/sonusEms/data/sys/ems.keystore -storetype
BCFKS -storepass sonusems
```

d. Restart the system:

```
/opt/sonus/ems/emsMgmt stop; /opt/sonus/ems/emsMgmt start
```

Customize the Logon Banner

Customize the **Logon Banner** by providing your text.

Start

1. Log on to the RAMP GUI using admin/admin as the username and password.
2. Navigate to **System > Settings > Logon Banner**. The **Logon Banner** window displays.
3. Update the message to display on the Logon page. The message allows up to 300 characters.
4. Update the banner content for JITC authentication. The banner allows up to 1500 characters.
5. Click **Apply** to save the updates.

Install Certificates on RAMP and the Browser

Perform the following procedure to install the certificates created in the above procedure, on RAMP and on the browser. Only on completion of these procedures, RAMP is JITC/FIPS enabled.

Prerequisites

- For the list of user and roles administration, refer to [Authentication and Authorization information on User Privileges in RAMP](#).
- Download the `clientuser.p12` and `cert-ourca.crt` files from the `JITC` directory.
- The `cert-ourca.crt` and `cacert.pem` certificates are available on the system where RAMP is accessed.

Start

1. Log on to the RAMP GUI using `admin/admin` as the username and password.
2. Navigate to **Management > Authentication & Authorization > Certificates**. The Certificates window displays.
3. Click **+ Add Certificate** to upload a certificate. For more information, refer to [Manage Certificates](#).
 - a. Upload the `cert-ourca.crt` and `cacert.pem` certificates.
4. From the web browser of your computer, import the certificates from the local machine.
5. On the RAMP GUI, the **Select a Certificate** window displays.
6. Select the certificate and click **OK**. The RAMP log on banner is displayed.
7. Accept the terms and click **OK**.
8. Log on to RAMP using your user name and password. The customized Logon banner is displayed.
9. Accept the terms and conditions displayed in the Logon banner and click **OK**.

Log on to JITC Enabled RAMP

After completing the previous procedures, perform the following procedure to log onto the JITC-enabled RAMP.

Prerequisites

- Perform all the procedures listed above.
- The client certificate is generated.
- Download the `clientuser.p12` and `cert-ourca.crt` files from the `JITC` directory.
- The `cert-ourca.crt` and `cacert.pem` certificates are available on the system where RAMP is accessed.
- The log on banner is customized.

Start

1. Log on to the RAMP GUI using your username and password. The customized Logon banner is displayed.
2. Accept the terms and conditions displayed and click **OK**.
3. You are now logged onto a JITC-enabled RAMP.

Configure RAMP for TLS Communication

This section explains configuring the Ribbon Application Management Platform (RAMP) for Transport Layer Security (TLS) communication.

Note

Refer to the SBC page [Security Configuration - TLS Profile](#) to configure TLS communication between FIPS/JITC enabled SBC and RAMP.

Note

For a geographically redundant (GR) RAMP, perform this procedure on both, the active and standby RAMPs.

Start

1. Import the SBC Certificate Authority (CA) certificate into the `ems.keystore` and `devmgmt-ms.truststore`.

- a. Log on as an `insight` user:

```
# su - insight
```

- b. Run the `manageCert` command:

```
$ /opt/sonus/ems/conf/cert/bin/manageCert import-othercert -n <sbcc name> -f <CA cert file>
```

2. Import the SBC CA cert into the `jssecacerts`:

- a. Log on as a `root` user.

- b. Import the SBC CA certificate into the `jssecacerts`:

```
# cp -p /opt/sonus/ems/jre/lib/security/jssecacerts /opt/sonus/ems/jre/lib/security/jssecacerts.original
# keytool -importcert -file <CA cert file> -alias <sbcc name> -keystore /opt/sonus/ems/jre/lib/security/jssecacerts -storetype BCFKS -storepass <password>
```

Note

If the intermediate CA cert file is available on the SBC, import it using the command:

```
# keytool -importcert -file <intermediate CA cert file> -alias <intermediate CA alias name> -keystore /opt/sonus/ems/jre/lib/security/jssecacerts -storetype BCFKS -storepass <password>
```

- c. Import the SBC CA certificate in to the License Manager (LM) truststore:

```
keytool -importcert -file <Root CA cert file> -alias <RootCAName> -keystore /opt/rbbn/lm/config/secure/lm-ms.truststore -storetype BCFKS -storepass <password>
```

Note

If the intermediate CA cert file is available on the SBC, import it using the command:

```
keytool -importcert -file <Intermediate CA cert file> -alias <IntermediateCAName> -keystore /opt/rbbn/lm/config/secure/lm-ms.truststore -storetype BCFKS -storepass <password>
```

3. Restart RAMP after the certificate is imported:

```
# su - insight -c '/opt/sonus/ems/emsMgmt stop; /opt/sonus/ems/emsMgmt start'
```

Configure NTP Server Authentication

Perform the following procedure to use authentication on the Network Time Protocol server:

Start

1. Perform the following procedure for the Server Configuration:
 - a. Update the configuration `/etc/chrony.conf` file:

```
allow x.x.x.x/yy <----- this should be device IP range
keyfile /etc/chrony.keys
```

- b. Specify the server-side key:

```
# vi /etc/chrony.keys
```

An example of the key file:

```
# Example of valid key:
1 SHA1 HEX:B2159C05D6A219673A3B7E896B6DE07F6A440995
```

- c. Restart the chrony service:

```
# systemctl restart chronyd.service
```

2. Perform the following for the client configuration:
 - a. Ensure that the client has the same key as the server in `/etc/chrony.keys` file.
An example:

```
# cat /etc/chrony.keys
1 SHA1 HEX:B2159C05D6A219673A3B7E896B6DE07F6A440995
```

- b. For example, if the key Id is 1, (as in the above example), the client's `chrony.conf` file must have a line in the following format:

```
server 192.168.122.33 key 1
```

Notifications

Any micro-service within the Ribbon Application Management Platform (RAMP) can use the optional Notifications service. To use it, the RAMP administrator adds the service manually after a RAMP installation.

When performing an EdgeMarc bulk action, specify whether you want to receive notifications for the action status.

Prerequisites

- The Notification service is deployed.

Note

- The bulk action Notification only displays if you enable the Notification option on an Edgemarc device Bulk action.
- Notifications gets purged after a specific configurable time.
- The Bell icon and Enable Notification field are visible only after configuring the notification service.
- The maximum number of notifications stored is limited for each user (1024 by default). Once the limit is reached, the old notifications are deleted. The Notification service properties are used to configure the limits.

Perform the following procedure to access the Notification list:

Start

1. Log on to RAMP GUI.
2. Click the Bell icon on the top right corner.
3. The **Notification** window appears with the following information.
 - a. List of notifications.
 - b. The Count of unacknowledged notifications.

Note

The count is displayed in the bell icon.

- c. Details of a particular notification.
 - d. Option to Acknowledge the notification.
 - e. Option to Acknowledge Bulk actions.
4. Use the following options to filter notifications:

Parameter	Description
Date/Time	The date and time interval at which you want to check the notifications.
Severity	The level of severity.
Type	The type of notification.
Source	The source from where the notification was initiated.
Summary	The summary provided.
Acknowledge	The list of Acknowledged and unacknowledged notifications.

5. Click the **Expand** button to get additional information about a notification. The "Description" and "Notification" details are displayed.
6. You can acknowledge a notification by clicking the **Acknowledge** button in an open notification row or by clicking the check icon in a closed one.

Note

To acknowledge multiple Notifications together, select the required notifications and click acknowledge from the Bulk action drop list.

Acknowledgements are accepted per user; if a notification goes to two users and only one acknowledges it, only one acknowledgment displays.

Security Best Practices

In this section:

- [RAMP Security Best Practices Introduction](#)
- [Managing RAMP Users and Accounts](#)
- [Managing RAMP Network Security](#)
 - [RAMP Secure Network Configuration](#)
- [Certificate Management](#)
- [RAMP Event Logging for Security](#)
 - [SFTP File Transfer Logs](#)

This guide provides information and procedures related to security practices on Ribbon Application Management Platform (RAMP).

RAMP Security Best Practices Introduction

In this section:

- [Security Concerns](#)
 - [Elevation of Privilege](#)
 - [Information Disclosure](#)
 - [Denial of Service](#)

Ribbon Application Management Platform (RAMP) is the element management system for the various Ribbon network elements. It provides full FCAPS (Fault, Configuration, Accounting, Performance, Security) management of those network elements. In many networks, RAMP must expose its northbound interface to untrusted networks, and so it is critical that RAMP be secured against potential attacks.

Security Concerns

RAMP has the same security concerns as any other Linux system if not properly secured. Since RAMP can have network interfaces on public networks, there is a risk of information disclosure, elevation of privileges, and denial of service attacks. The standard security best practices for any Linux system apply to RAMP as well. RAMP has various ports which are open which must be secured, and RAMP ships with all open ports featuring some security in place.

Elevation of Privilege

Privilege escalation is when a normal user can gain access to more permissions than he should have. For example, the user can gain access to the same or similar permissions to the root user.

The primary way to avoid privilege escalation is to secure the Linux user accounts and making sure that all software is running the latest versions.

RAMP periodically ships maintenance releases which include the latest security patches for the Linux operating system and the RAMP application itself. Ribbon recommends that customers upgrade RAMP to the latest maintenance release on the particular release stream that they are running to minimize security vulnerabilities. In addition, we recommend the following:

- During RAMP installation, the user is prompted to change the default password for root. Choose a hard-to-guess password with sufficient complexity and length as per the standard Linux recommendations for setting passwords.
- RAMP user passwords are set to expire every 90 days, and the user will be prompted to change them 7 days before they are set to expire. You can also update that parameter to a smaller value as required by your own corporate security standards.
- You must not enable SSH access for the root user (this is disabled by default and should not be re-enabled).

Information Disclosure

Potential sources for information disclosure is by accessing the data via one of the northbound interfaces (UI, API, CLI).

All of the northbound interfaces are secured via username / password credentials, and so those credentials must be managed in a secure fashion. Users should work to properly secure their own passwords and follow standard recommendations on proper storage and management of passwords (e.g. users should not share passwords with others or write them down, etc.). In addition, if access to RAMP should only be allowed from certain networks (internal for example), then firewalls should be used to limit access to those interfaces on RAMP.

Denial of Service

Denial of service attacks against RAMP will not impact call processing capabilities of the other Ribbon network elements, but it can certainly impact a user's ability to monitor the network. RAMP doesn't have any denial of service protections other than those provided in the Linux operating system and the Apache web server. The best way to determine that a DoS attack is happening is by monitoring the standard Linux logs as well as the Apache web server logs.

Managing RAMP Users and Accounts

In this section

- [Use a Master-Key to Encrypt RAMP Passwords](#)
- [Follow Standard Linux Password Guidelines](#)
- [Change Any Default Passwords](#)
- [Manage Administrative Accounts](#)
- [Avoid Customization of the Linux Environment](#)

The following security guidelines apply when managing Ribbon Application Management Platform (RAMP) user accounts.

Use a Master-Key to Encrypt RAMP Passwords

Periodically generate a master-key to encrypt RAMP passwords.

Refer to [Generate a Master Key to Encrypt RAMP Passwords](#).

Follow Standard Linux Password Guidelines

Protect your password

Don't write down your password - memorize it. In particular, don't write it down and leave it anywhere, and don't place it in an unencrypted file. Use unrelated passwords for systems controlled by different organizations. Don't give or share your password, in particular to someone claiming to be from computer support or a vendor. Don't let anyone watch you enter your password. Use the password for a limited time and change it regularly.

Choose a hard-to-guess password

The Linux command to change passwords ("passwd") through the calls to the pam_cracklib PAM module will try to prevent you from choosing a really bad password, but it isn't foolproof; create your password wisely. Don't use something you'd find in a dictionary (in any language or jargon). Don't use a name (including that of a spouse, parent, child, pet, fantasy character, famous person, and location) or any variation of your personal or account name. Don't use accessible information about you (such as your phone number, license plate, or social security number) or your environment. Don't use a birthday or a simple pattern (such as backwards, followed by a digit, or preceded by a digit. Instead, use a mixture of upper and lower case letters, as well as digits or punctuation. When choosing a new password, make sure it's unrelated to any previous password. Use long passwords (say at least 8 characters long). You might use a word pair with punctuation inserted, a passphrase (an understandable sequence of words), or the first letter of each word in a passphrase.

These principles are partially enforced by the system, but only partly so. Vigilance on your part will make the system more secure.

Change Any Default Passwords

RAMP has system-level user accounts and application-level user accounts. Some of those accounts have default passwords. For security purposes, it is highly recommended that any default passwords be changed to something more secure.

For user account names, default passwords, and how to change those passwords; refer to [Manage RAMP Account Names and Passwords](#).

Manage Administrative Accounts

Administrative accounts should be defined and managed in accordance with your organization's security posture. The following is a recommended best practice:

- Do not share accounts between individuals.
- Provide each individual with an account consistent with their role.
- Minimize access to Linux passwords.

Avoid Customization of the Linux Environment

Do not make changes to the embedded Linux operating environment unless they are reviewed and authorized by Ribbon. This includes:

- Addition of new packages
- Changes to existing packages
- Operational changes such as crontab updates

Managing RAMP Network Security

In this section:

- [RAMP Secure Network Configuration](#)
 - [RAMP Security Group Rules](#)
 - [RAMP Ports Descriptions](#)
 - [RAMP Ports Descriptions for EdgeView](#)

Ribbon highly recommends to place all the network elements that talk to Ribbon Application Management Platform (RAMP) in a trusted network.

RAMP Secure Network Configuration

In this section:

- [RAMP Security Group Rules](#)
- [RAMP Ports Descriptions](#)
- [RAMP Ports Descriptions for EdgeView](#)

Along with the standard ports for various protocols, there are many other system ports that are open by default for all these communications on Ribbon Application Management Platform (RAMP).

It is recommended to control access to these ports to secure the equipment and data. Use an external firewall as needed.

For more information on ports and their purpose on RAMP, refer to [RAMP Ports Descriptions](#).

RAMP Security Group Rules

This page describes the summary of all the ports used in Ribbon Application Management Platform (RAMP) on cloud. The ports are specific to an application or a feature and are only applicable when in use.

In the cloud environment, these ports are allowed in the security group associated with the instance type. The various fields are described in the table below.

Security Rule Field Descriptions

Field	Description
Direction (initial)	For UDP, this is both directions. For TCP, this is Outbound for clients and inbound for servers (to match the direction of the initial connection). NOTE: This definition matches the way firewall rules are defined.
Ether Type	It is either IPv4 or IPv6. Separate rules are supplied when both IPv4 and IPv6 are supported.
IP Protocol	UDP or TCP.
Local Port	An exact port number, or a wildcard. TCP clients usually use an ephemeral local port is wildcarded.
Local IP/interface	The local interface or internal object (such as SIP SP).
Remote Port	An exact port number, or a wildcard. TCP clients usually use an ephemeral local port which is wildcarded.
Remote Peers	Peer type. Use this to set the most constrained remote network prefix.

The following table provides security rules for the RAMP.

Note

The rules apply to both IPv4 and IPv6.

RAMP Security Rules

Direction (Initial)	IP Protocol	Local Port	Local IP/Interface	Remote Port	Remote Peers	Notes
Ingress	TCP	22	Mgt	*	SSH clients	SSH connection
Egress	TCP	*	Mgt	22	PSX, RAMP, SBC	SSH connection (tunneled protocols such as PIPE, and so on.) SBC for SBC CLI proxy.

Direction (Initial)	IP Protocol	Local Port	Local IP/Interface	Remote Port	Remote Peers	Notes
Egress	UDP	*	Mgt	53	DNS server	Post-paid registration and usage reporting URLs.
Both	UDP	123	Mgt	123	NTP server	NTP
Both	UDP	161	Mgt	161	PSX, SBC	SNMP polling
Both	UDP	162	Mgt	162	PSX, SBC	SNMP traps
Ingress	TCP	443	Mgt	*	RAMP client	RAMP GUI Access (HTTPS)
Egress	TCP	*	Mgt	443	SBC, SBC Configurator	SBC Manager, REST calls to SBC or SBC Manager
Egress	TCP	*	Mgt	444	SBC	
Egress	UDP/TCP	514	Mgt	514		rsyslog (either UDP or TCP depending on the remote rsyslog host)
Egress	UDP	*	Mgt	1812	Radius Server	Radius Authentication port (configurable - this is the default).
Egress	UDP	*	Mgt	1813	Radius Server	Radius Accounting port (configurable - this is the default).
Egress	TCP	*	Mgt	2022	SBC, SBC Configurator	NETCONF Session to SBC Configurator and SBC
Egress	TCP	*	Mgt	2024	SBC, SBC Configurator	SFTP to SBC, SBC Configurator
Both	UDP	5200	Mgt	*	SNMP agent	SNMP - Agent Trap Forwarder

Direction (Initial)	IP Protocol	Local Port	Local IP/Interface	Remote Port	Remote Peers	Notes
Both	TCP	5432	Mgt	5432	RAMP	PostgreSQL listener process on remote RAMP (redundancy)
Both	TCP	6432	Mgt	6432	RAMP	Pgbouncer
Egress	TCP	*	Mgt	6462	PSX	RAMP and PSX communication (SFTP stats collection) using REST
Ingress	TCP	6462	Mgt	*	RAMP	RAMP SFTP stats collection from remote RAMP (using REST)
Both	TCP	6700	Mgt	6700	RAMP	OpenSAF
Both	TCP	6900	Mgt	6900	RAMP	OpenSAF
Ingress	TCP	8122	Mgt	*	CLI client	SSH CLI (for provisioning the PSX by CLI)
Egress	TCP	*	Mgt	8890	DSC	Inventory Audit port
Both	UDP	9004	Mgt	*	PSX	PSX call trace
Both	TCP	9092	Mgt	9092	RAMP	Kafka
Egress	TCP	*	X1 intf	15005	SS8 Server	(SS8-based LI Only) X1 configuration interface to SS8 (non-secure). The port-numbers may differ. Obtain the actual port-number provided by SS8. NOTE: Do not use non-secure ports. Use secure ports instead.

Direction (Initial)		IP Protocol		Local Port	Local IP/Interface	Remote Port	Remote Peers	Notes		
Egress		TCP		*	X1 intf	55700	SS8 Server	(SS8-based LI Only) X1 configuration interface to SS8 (secure). The port-numbers may differ. Obtain the actual port-number provided by SS8.		
Ingress		TCP		19991	Mgt	*	RAMP	Sonus agent configuration		
Egress		TCP		*	Mgt	19991	PSX, RAMP	Sonus agent configuration		
Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
RAP (Ribbon Audit Portal)	Egress	TCP	443	HTTPS	License Manager	IPv4 / IPv6	Used by the License Manager process to upload postpaid reports to RAP.	IPv4 / IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open

Optional ports on RAMP

This section covers ports supported for optional services on the **RAMP**. Open these ports on your private/public cloud instances to use the optional services.

RAMP security rules for optional services

Direction (Initial)	Ether Type	IP Protocol	Local Port	Local IP/Interface	Remote Port	Remote Peers	Notes
Egress	IPv4/v6	TCP	8080	Mgt		STI	The port to use for the STI service.

Direction (Initial)	Ether Type	IP Protocol	Local Port	Local IP/Interface	Remote Port	Remote Peers	Notes
Egress	IPv4/v6	TCP	2379	Mgt		etcd VMs	The port to connect to etcd instances for RAMP GR monitoring.

RAMP Ports Descriptions

In this section:

- [RAMP Ports](#)
- [ETCD VM Ports](#)

The Ribbon Application Management Platform (RAMP) listens to the network ports in the following table. Some ports are unavailable if the corresponding product features are not configured.

RAMP Ports

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
SSH client	Ingress	TCP	22	SSH	sshd	IPv4/IPv6	Secure login from the console terminal to the RAMP through SSH.	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
Send mail client on RAM	Ingress	TCP	25	SMTP	mail agent	IPv4/IPv6	Simple Mail Transfer Protocol (SMTP), used for user-level client mail applications , sends email notifications .	IPv4(loopback i/f:127.0.0.1)	IPv4/IPv6 address of the peer	Only open for traffic from loopback and local IP address.
DHCP Server	Ingress	UDP	68	DHCP	dhclient	IPv4	DHCP for IPv4 cloud instances.	IPv4 address of the RAM	IPv4 address of the peer	Open for IPv4 deployments
NTP server	Both	UDP	123	NTP	ntpd	IPv4/IPv6	Network Time Protocol for clock synchronization.	IPv4/IPv6 address of the RAM	IPv4/IPv6 address of the peer	Always open

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
RAMP GR system	Both	UDP	161	SNMP	Agent	IPv4/IPv6	SNMP reachability polling for the RAMP node. The RAMP GR also uses it to monitor the Agent on the other host.	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open
Any Ribbon device	Both	UDP	162	SNMP	FM Trap Receiver	IPv4/IPv6	SNMP Event notification V2 trap from other devices to the RAMP.	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open
HTTP clients	Ingress	TCP	443	HTTPS	Apache httpd	IPv4/IPv6	Redirects requests to the JBoss application server. The RAMP Web GUI, SOAP and REST APIs. Note: EdgeMarc and Edge Devices will contact the RAMP on port 443.	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
RAP (Ribbon Audit Portal) ZTP	Egress	TCP	443	HTTPS	License Manager Edge View service (EV service)	IPv4/IPv6	Used by the License Manager process to upload postpaid reports to RAP. Fetch C2E during Swe Edge registration and auto provisioning of EdgeMarc devices.	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open
Syslog server	Both	UDP	514	syslog	rsyslogd	IPv4/IPv6	syslogd	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	
DHCP server	Ingress	UDP	546	DHCP	dhclient	IPv6	DHCP	IPv6 address of the RAMP	IPv6 address of the peer	Open for IPv6 deployments

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
Local RAM P	Both	UDP	1610	SNMP	snmpd	IPv4/ IPv6	SNMP listener fetches hardware-level traps and sends them to the Agent.	IPv4 address of the RAM P	IPv4/ IPv6 address of the peer	
RAM P GR	Both	TCP	5000	HTTPS	DBaaS Service Monitor or REST API	IPv4/ IPv6	DBaaS Service Monitor REST API.	IPv4/ IPv6 address of the RAM P	IPv4/ IPv6 address of the peer	Always open
HTTP Client	Both	UDP	5200	SNMP	Agent	IPv4/ IPv6	Agent Trap Receiver Port used for receiving the hardware traps sent from port 1610.	IPv4/ IPv6 address of the RAM P	IPv4/ IPv6 address of the peer	Always open

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
Local RAMP/GR system	Ingress	TCP	5432	PostgreSQL proprietary	Postgres	IPv4/IPv6	PostgreSQL database – internal DB connections and connections for RAMP/GR.	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open
Device, RAMP	Ingress	TCP	5671	AMQP	nginx docker container	IPv4/IPv6	For establishing a communication channel between RAMP and device (EMPath).			
Local RAMP/GR system	Ingress	TCP	6432	PostgreSQL proprietary	Postgres	IPv4/IPv6	PostgreSQL database – internal DB connections and connections for the RAMP/GR.	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open
local RAMP	Ingress	TCP	6462	HTTPS	Agent	IPv4/IPv6	Used to enable FTP statistics collection from the RAMP.	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
Local RAMP/GR system	Ingress	TCP	6700	OpenSAF proprietary	OpenSAF	IPv4/IPv6	RAMP/GR Redundancy	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open
Local RAMP/GR system	Ingress	UDP	6800	OpenSAF proprietary	OpenSAF	IPv4/IPv6	RAMP/GR Redundancy	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open
Local RAMP/GR system	Ingress	UDP	6900	OpenSAF proprietary	OpenSAF	IPv4/IPv6	RAMP/GR Redundancy	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
RAMP	Ingress	TCP	8022	ssh	sshd process running inside the docker services container	IPv4/IPv6	Device Open GUI functionality from the RAMP			
STI	Egress	TCP	8080	SSH	sshd	IPv4/IPv6	The port to use for the STI service.	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always Open
RAMP	Ingress	TCP	8081	HTTP	Kafka Schema Registry port	IPv4/IPv6	FM service			
CLI Client	Ingress	TCP	8122	SSH	RAMP	IPv4/IPv6	Remote access to the RAMP CLI from client to RAMP through SSH.	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Open only if the RAMP-CLI license is deployed in the Ribbon-provided Dell Server.

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
RAM P	Ingress	TCP	8444	http	nginx docker container	IPv4/IPv6	Device Open GUI functionality from RAMP.			
Client desktop running PSX Manager	Ingress	TCP	9001	Ribbon proprietary	RAMP	IPv4/IPv6	Client/Server Communication from PSX Manager to RAMP through PSX proxy server over https (SSL).	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open
PSX	Ingress	UDP	9004	Ribbon proprietary	Call Trace Listener	IPv4/IPv6	Call Trace event notification from other devices to RAMP.	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	
Local RAMP/GR	Ingress	TCP	9092	Kafka proprietary	Kafka	IPv4/IPv6	Kafka	IPv4/IPv6 address of the RAMP	IPv4/IPv6 address of the peer	Always open

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
HTTP Client	Ingress	TCP	9992 (disabled by default)	HTTP	RAM P	IPv4/IPv6	JBoss Management Console.	IPv4/IPv6 address of the RAM P	IPv4/IPv6 address of the peer	
OBS Probe	Ingress	TCP	13313	HTTP		IPv4/IPv6	To observer health check.	IPv4/IPv6 eth0 address of the OBS		Always open
RAM P/GR	Ingress	TCP	19991	HTTPS	Agent	IPv4/IPv6	To perform the device and agent configuration: - Setting trap destinations - Set SNMP read/write community strings. - JMX communication from the RAM P to device agent.	IPv4/IPv6 address of the RAM P	IPv4/IPv6 address of the peer	Always open

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
OBS Probe	Ingress	TCP	9101	HTTP	otelcol	IPv4/IPv6	This is a Prometheus port.	IPv4/IPv6 eth0 address of the OBS		Always open
RAMP	Egress	TCP	2379	HTTP		IPv4/IPv6	RAMP (client) to ETCD (server) Communication. Use GRPC protocol.			

ETCD VM Ports

Peer Type	Direction	Transport Protocol	Client Port	Server Port	Optional / Mandatory	Usage
ETCD Peer	Ingress	TCP	Ephemeral	2380	Mandatory	ETCD Peer Server to ETCD Local Server Communication (Ingress)
ETCD Peer	Egress	TCP	Ephemeral	2380	Mandatory	ETCD Local Server to ETCD Peer Server Communication (Egress)
RAMP	Ingress	TCP	Ephemeral	2379	Mandatory	RAMP (client) to ETCD (server) Communication. Use GRPC protocol.
ETCD Peer	Ingress	TCP	Ephemeral	2379	Mandatory	Used between 2 ETCD servers during installation Use GRPC protocol.

Peer Type	Direction	Transport Protocol	Client Port	Server Port	Optional / Mandatory	Usage
ETCD Peer	Egress	TCP	Ephemeral	2379	Mandatory	ETCD Local Server to ETCD Peer Server Communication (Egress)
VM Access	Ingress	TCP	Ephemeral	22	Mandatory	SSH access to VM
Prometheus Client (Scrape) used for Node-Exporter metrics	Ingress	TCP	Ephemeral	9100	Optional	A remote Prometheus client can get Metrics generated by the server (CPU, memory, ...)
Prometheus Client (Scrape) used for Fluentbit Metrics	Ingress	TCP	Ephemeral	24231	Optional	A remote Prometheus client can get Metrics generated by Fluentbit

RAMP Ports Descriptions for EdgeView

Ribbon Application Management Platform (RAMP) listens to the network ports listed in the following table. Some of these ports are not available if the corresponding product features are not configured.

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
Device, RAMP	Ingress	TCP	5671	AMQP S	nginx docker container	IPv4/IPv6	For establishing communication channel between RAMP and device (EMPath).	IPv4/IPv6 addresses of RAMP	IPv4/IPv6 address of SBC Swe Edge, SBC 1000, and SBC 2000.	Open when the EV service is deployed.

Peer Type	Direction	Transport Protocol	Local Port	Application Level Protocol	Process Name	Ether Type	Usage	Local IP/Interface	Remote Peers	iptables rule
RAMP	Ingress	TCP	8022	ssh	sshd process running inside docker services container	IPv4/IPv6	Device Open GUI functionality from the RAMP.	IPv4/IPv6 addresses of RAMP	IPv4/IPv6 address of SBC Swe Edge, SBC 1000, and SBC 2000.	Open when the EV service is deployed
RAMP	Ingress	TCP	8444	http	nginx docker container	IPv4/IPv6	Device Open GUI functionality from RAMP.	IPv4/IPv6 addresses of RAMP	IPv4/IPv6 addresses of the systems which connect to RAMP GUI using a web browser.	Open when the EV service is deployed

Certificate Management

Ribbon Application Management Platform (RAMP) ships with two default certificates which are self-signed and are not recommended for production use. One certificate is used for the https connections to RAMP (on ports 443 / 9001), and the other certificate is used to secure the https connection to the Agent (running on port 19991).

It is highly recommended that customers replace all of the default certificates shipped with RAMP with production certificates signed by a recognized certificate authority.

The procedures for replacing the certificates can be found here:

- [Secure Login to the RAMP GUI](#)
- [Secure Communication Between RAMP and Devices](#)

RAMP Event Logging for Security

In this section

- [System Activity Logs](#)
- [User Activity Logs](#)
- [Web Request Logs](#)
- [API and CLI Usage Logs](#)
- [Remote Syslog](#)

Related articles:

- [SFTP File Transfer Logs](#)

Ribbon Application Management Platform (RAMP) has a variety of log files which store information on user and system activity that can be reviewed from a security perspective.

System Activity Logs

The primary log file for all application related logging is `/opt/sonus/ems/weblogic/sonusEms/logs/sys/ems_trace_log`.

If you see any errors in the system, it is likely that some detail will be found in this log file. You can view the system activity log on the **RAMP** GUI without logging into the Linux shell. It could be useful when you are debugging errors that may have resulted from unauthorized access.

For more information, refer to [System Activity Logging](#).

User Activity Logs

RAMP tracks all application user activity when the user is logged into the system. This information is not logged to the disk but instead stored in the database. This log is useful to track who made configuration changes, especially if you are suspicious that someone has gained unauthorized access to the system.

For more information, refer to [Monitor User Activity](#).

In addition, all failed logins to the **RAMP** UI are tracked here:

`/var/log/ems/ems_login.log`

Web Request Logs

Although the file is very verbose, **RAMP** has a log file which tracks every single web request to **RAMP**, including the source IP where the request originated from. It is the standard Apache httpd log, and it can be found in `/var/log/httpd`. The log file is called `access_log`, and it is archived and compressed when the log file exceeds the threshold. The `access_log` file is accessible only to root users on **RAMP**.

API and CLI Usage Logs

If you want to track the usage of **RAMP** APIs or actions on the command line, you can find the information on all access to those in the following files:

- API security-related information (including failed logins):
`/opt/sonus/ems/weblogic/sonusEms/logs/sys/api_security_log`
- Command line security-related information (including failed logins):
`/var/log/ems/ems_login.log`
- RAMPAPI provisioning operations:
`/opt/sonus/ems/weblogic/sonusEms/logs/sys/emsapi_prov_log`
- RAMP command-line provisioning operations:
`/opt/sonus/ems/weblogic/sonusEms/logs/sys/ems_cli_log`

Remote Syslog

RAMP supports sending the most critical logs to a remote Syslog server. This is highly recommended as this means the logs are stored externally. There are two types of logs which can be streamed to a remote Syslog server: security-specific logs and the primary **RAMP** application log (`ems_trace_log`). Within the **RAMP** GUI you can specify the remote Syslog server IP address to enable remote Syslog logging.

For more information on enabling remote Syslog, refer to [Exporting Logs to a Remote Syslog Server](#).

SFTP File Transfer Logs

The file transfers using SFTP protocol are logged in the file *sftp.log* available at */var/log/*.

Only the root user on Ribbon Application Management Platform (RAMP) can access the *sftp.log* file.

Up to 10 *sftp.log* files (1 MB each) are stored. When the size of file reaches 1 MB, the file is compressed in gzip format. When the number files reach the threshold, older files are overwritten.

The following is an example the *sftp.log* file:

```
May 25 06:15:26 vinaydeepems11a016 sftp-server[1519]: session opened for local user root
from [10.70.52.206]
May 25 06:15:26 vinaydeepems11a016 sftp-server[1519]: received client version 3
May 25 06:15:57 vinaydeepems11a016 sftp-server[1519]: opendir "/opt/sonus/ems/"
May 25 06:15:57 vinaydeepems11a016 sftp-server[1519]: closedir "/opt/sonus/ems/"
May 25 06:15:57 vinaydeepems11a016 sftp-server[1519]: realpath "/opt/sonus/ems/"
May 25 06:16:43 vinaydeepems11a016 sftp-server[1519]: open "/opt/sonus/ems/
emsRestart.log" flags READ mode 0666
May 25 06:16:43 vinaydeepems11a016 sftp-server[1519]: close "/opt/sonus/ems/
emsRestart.log" bytes read 40838 written 0
May 25 06:17:00 vinaydeepems11a016 sftp-server[1519]: session closed for local user root
from [10.70.52.206]
```

- May 25 06:15:26
Indicates the time of the transfer.
- vinaydeepems11a016
Indicates the host name of RAMP.
- [1519]
Indicates the process ID (PID).
- session opened for local user root from [10.70.52.206]
Indicates the details of the activity.
The details include:
 - [10.70.52.206]
the client server IP address
 - opendir
directory opened
 - closedir
directory closed
 - realpath
location of the directory or file

Configuring RAMP Redundancy

In this section:

- [Generate Redundancy Templates](#)
- [Configuring RAMP GR](#)
- [Configuring RAMP GR with Automatic Switchover Enabled](#)
 - [Setting Up an etcd Cluster](#)
 - [etcd Alerts](#)
 - [List of Traps and Alerts](#)
 - [Updating the SNMP trapTarget](#)
 - [RAMP etcd System Requirements](#)

Related articles:

- [Deployment Models](#)
- [Managing Redundancy](#)

Ribbon Application Management Platform (RAMP) supports configuring geographical redundancy (GR) between two RAMP devices.

A GR deployment on RAMP begins as two RAMP standalone devices at different geographical locations that you configure to work together in a GR fashion. The RAMP device at one of the GR sites functions as a "source" or active RAMP node and the other functions as a "target" or standby RAMP node. You can run the GR configuration procedure on either standalone RAMP node, but note that the device on which you configure GR becomes the source RAMP node. The process involves using a template file in which you set parameters for the deployment.

After GR is configured, there is constant replication of data from the source RAMP to the target RAMP. If the source RAMP goes down, you can perform a failover from the target RAMP. Similarly, you can also do a switchover and change the source and target roles. If necessary, you can also teardown the GR setup and resume having two standalone RAMP devices. If one device fails, you have the option to replace it with a new device. Refer to [Managing Redundancy](#) for information on monitoring the deployment and management procedures. Refer to [Configuring RAMP GR](#) for information on setting up a standard GR deployment.

As an alternative to initiating manual switchovers, RAMP also supports a deployment model that enables automatic switchover between GR instances. To enable automatic switchover, you must deploy three additional VMs, each running an instance of etcd. The etcd instances continually monitor whether they are able to communicate with the RAMP instances and use that information to function as arbitrators that determine which RAMP instance should be active. A switchover occurs automatically when a majority of the etcd instances determine that the current active instance is no longer reachable. Refer to [Configuring RAMP GR with Automatic Switchover Enabled](#) for more information on switchover processing, the resources required to implement automatic switchover, and how to deploy etcd.

Generate Redundancy Templates

Related articles:

- [Deployment Models](#)
- [Configuring RAMP GR](#)
- [Managing Redundancy](#)
- [Configuring RAMP GR with Automatic Switchover Enabled](#)

Use the script `RDbuild_config.sh` to generate a redundancy template for a Ribbon Application Management Platform (RAMP) geographically redundant (GR) deployment. You use the redundancy template when you [configure RAMP for GR](#) to configure redundancy parameters for the deployment.

Note

The following procedure describes creating a template for a standard GR deployment in which switchovers are triggered manually. RAMP also supports a deployment model that enables automatic switchover between GR instances. To enable automatic switchover, you must deploy three additional VMs, each running an instance of etcd. You also specify different redundancy template parameters to enable automatic switchover. Refer to [Configuring RAMP GR with Automatic Switchover Enabled](#) for more information.

Start

1. On the RAMP device that you intend to use as the source/active node in the GR deployment, SSH to the RAMP CLI as the `admin` user.
2. Change to the `root` user:

```
sudo su -
```

3. Enter the following command:

```
/etc/sonus/RDbuild_config.sh -o /<directory for the template>/<name for the template>.conf -g <the redundancy model>:<IP schema>
```

The following is an example that generates the redundancy template file in the `/opt` directory. See the first table below for more information on the script's parameters.

```
/etc/sonus/RDbuild_config.sh -o /opt/GR.conf -g gr:ipv4
```

4. Edit the generated template file to suit your deployment. Use the second table below for more information on the parameters in the redundancy template.
5. After you create your redundancy template file, refer to [Configuring RAMP GR](#) for the procedure to configure your GR deployment.

Reference Tables

As shown in step 3, the basic format for the script is: `RDbuild_config.sh -o <name for the template> .conf -g <the redundancy model> : <IP schema>`

The following table describes the parameters you can use with the script, including optional parameters.

RDbuild_config.sh Parameters

Parameter	Optional (O) / Mandatory (M)	Description
-o	M	Use to specify the file name of the configuration file. Use this option along with the <code>-g</code> option.
-g	M	Use to generate a cluster configuration template using the specified redundancy model and IP schema.
<the redundancy model>	M	Specifies the redundancy model. Currently, <code>gr</code> is the supported redundancy model.
<IP schema>	M	The IP address schema. Enter one of the following: <code>ipv4</code> for an IPV4 network <code>ipv6</code> for an IPv6 network
oss	O	Use, in the following format, to enable the option to send SNMP traps concerning GR status to an Operations Support Systems (OSS). <code>RDbuild_config.sh -o <name for the template>.conf -g <the redundancy model> : <IP schema>:oss</code>
-h	O	Use to list the help information for the script.

The following table describe the parameters you can configure in the redundancy template.

Redundancy Template Configuration Parameters

Parameter	Description	Value
Fixed Settings		
<code>_primaryServer</code>	The IP address of the RAMP active node. The IP address of the node in which the cluster set-up was initiated.	A valid IP address

Parameter	Description	Value
_clusterName	The name of the cluster.	Alphanumeric characters
_numSites	The number of sites in the cluster	• 2: For GR
_numNodes	The number of nodes in a site.	• 1: For GR
_totalNodes	The total number of nodes in the cluster.	• 2: For GR
_ipschema	The IP address mode.	• ipv4 • ipv6
_pm_export_sync_to_standby	The flag to set sync of pm export reports.	• true: enable report sync. • false: disable report sync.
_site<site number>_name	The name for site <site number>.	Alphanumeric characters
_site<site number>_vip_v4prefix	The length of the virtual IPv4 address prefix for the site.	integer
_site<site number>_vip_v6prefix	The length of the virtual IPv6 address prefix for the site.	integer
_oss_info	The flag to configure Operations Support Systems (OSS) on the RAMP.	yes: Enables OSS no: Disables OSS
_oss_ip	The IP address of the OSS system. Discard this parameter if _oss_info is set to "no".	A valid IP address

Parameter	Description	Value
_oss_snmp_port	Discard this parameter if _oss_info is set to "no". The SNMP port number of the OSS system.	A valid port
_oss_snmp_community_str	Discard this parameter if _oss_info is set to "no". The SNMP community string of the OSS system.	Alphanumeric characters
Node		
_node<node number>	The host name of the node <node number>.	Alphanumeric characters
_node<node number>_id	The sequence number of node <node number>.	• 1 • 2
_node<node number>_ip	The IP address of node <node number>.	A valid IP address
_node<node number>_site	The site name of node <node number>.	Alphanumeric characters

Configuring RAMP GR

Related articles:

- [Managing Redundancy](#)
- [Generate Redundancy Templates](#)
- [Configuring RAMP GR with Automatic Switchover Enabled](#)

Use the following procedure to configure a geographically redundant (GR) Ribbon Application Management Platform (RAMP) deployment. Prior to running the procedure you must generate a redundancy template file to specify configuration details for the deployment. Refer to [Generate Redundancy Templates](#).

Run the procedure on the RAMP device that you want to be the source/active node for the GR deployment. It is not necessary to repeat the setup on the target/standby device.

RAMP GR is supported in KVM, VMware, and OpenStack environments.

Note

The following procedure describes configuring a standard GR deployment in which switchovers are triggered manually. RAMP also supports a deployment model that enables automatic switchover between GR instances. To enable automatic switchover, you must deploy three additional VMs, each running an instance of etcd. You also specify different redundancy template parameters to enable automatic switchover. Refer to [Configuring RAMP GR with Automatic Switchover Enabled](#) for more information.

Prerequisites

- Two RAMP devices are up and running in the same environment with the same version.
- If the optional EdgeView (EV) service that enables managing SBC Edge devices is deployed, it should be deployed on both RAMP devices.
- For RAMP on KVM/VMware, the two RAMP devices are running on separate host servers.
- The standby device is accessible from the active device, and vice versa.

Note

If you have restored the database on an OpenStack deployment, password-less SSH from the active RAMP device to the standby RAMP device (and vice versa) is not possible until GR is configured.

- You can ping the standby device from the active device and you can ping the active device from the standby device.
- The same password is set for the `admin` and `insight` users on the active and standby devices.

Note

The `insight` password is reset in the RAMP active device after restoring the database (with the password of the old database).

- If cron entries are created manually on the RAMP active device, you must also create the same cron entries on the standby device. In RAMP GR, cron entries are not copied and synchronized from active to standby, or vice versa.
- Ensure you have the redundancy template file generated for the deployment. Refer to [Generate Redundancy Templates](#).
- Before you run the `RDsetup.sh` command, modify the session timeout interval and set it to zero (0) by performing the procedure at [Modify User Session Timeout Interval](#). After you modify the session timeout interval, re-initiate a new SSH session and then run the `RDsetup.sh` command.

Start

1. On the RAMP device you want to establish as the source/active node in the GR deployment, log onto the CLI as the `admin` user.
2. Change to the `root` user:

```
sudo su -
```

3. Enter the following command, specifying the path and name for the redundancy template file generated for your GR deployment:

```
/etc/sonus/RDsetup.sh <absolute path to the redundancy template file>
```

The following is an example that specifies a redundancy template file, `GR.conf`, in the `/opt` directory.

```
/etc/sonus/RDsetup.sh /opt/GR.conf
```

Example

```
[16:17:41] Starting redundancy cluster setup .....  
[16:17:42]  
Building RD configuration locally .....  
Please enter Password of admin user for all nodes (press ENTER if not needed) ->  
admin
```

4. Enter the `admin` password:

Note

If you are configuring a GR deployment on OpenStack and the password-less authentication for the `admin` user from the active RAMP device to the standby RAMP device is enabled, press ENTER.

The script completes setting up GR and the RAMP processes start shortly.

5. Change to the `insight` user to run a status check to verify that the system is healthy:

```
su - insight
```

6. Enter the following to check the RAMP status:

```
/opt/sonus/ems/emsMgmt status
```

7. Log onto the CLI of the standby RAMP device as the `admin` user.
8. Change to the `insight` user:

```
sudo su - insight
```

9. Enter the following to check the status on the RAMP standby node:

```
/opt/sonus/ems/emsMgmt status
```

10. Restore the session timeout interval to 750 by performing the procedure at [Modify User Session Timeout Interval](#).

Note

If the configuration process is interrupted and you resume `RDsetup.sh`, the RAMP offers the following option:

```
Record showing the <script name> script was being executed and was not completed.
Do you want to resume the operation from the previous point of failure (yes|no)?.
```

Perform one of the following:

- Enter "yes" to resume the operation from the point of failure.
- Enter "no" to execute the script again. The RAMP shows the following message:

```
Do you want to proceed with a fresh new operation (yes|no)? ->
```

Perform one the following:

- Enter "yes" to execute the script.
- Enter "no" to terminate the session.

Note

All micro services certificates present on the primary RAMP are copied to the target RAMP containing the CN and SAN details for the primary RAMP.

Configuring RAMP GR with Automatic Switchover Enabled

In this section:

- [Generate a Redundancy Template](#)
- [Configure RAMP GR Parameters](#)

Related articles:

- [Setting Up an etcd Cluster](#)
- [Deployment Models](#)
- [Configuring RAMP Redundancy](#)
- [Managing Redundancy](#)
- [RAMP CNF - Resiliency](#)

As an alternative to initiating manual switchovers, Ribbon Application Management Platform (RAMP) supports a deployment model that enables automatic switchover between geographically redundant (GR) instances. To enable automatic switchover, you must deploy three additional virtual machines (VMs) to monitor the RAMP GR

deployment. You must allocate an IP address to each VM. Also, ensure each VM is running an instance of etcd. Refer to [Setting Up an etcd Cluster](#) for the procedures to deploy the necessary VMs.

In a typical GR deployment, RAMP instances are deployed at two separate geographic sites. To enable automatic switchover, a VM running etcd is deployed at each RAMP site and at a third, “neutral” site. Together, the three etcd instances determine which RAMP instance is active.

RAMP GR is configured to use the etcd instances to select which RAMP instance is the active or “leader” instance. Before electing a site as the leader, etcd requires that the potential active instance achieves a “quorum” from the etcd instances. The concept of a quorum applies to the etcd cluster layer wherein at least two etcd nodes are needed to maintain a quorum amongst the etcd nodes in an etcd cluster.

Subsequently, if the standby RAMP instance finds it cannot communicate with the active RAMP, it communicates with etcd to see if the active RAMP is still reachable. As long as the active RAMP communicates with at least one etcd node and that etcd node has a quorum with the peer etcd nodes, no auto-switchover occurs. If fewer than two etcd nodes (one etcd node) communicate with the active RAMP, and the only etcd node that communicates with the active RAMP loses the quorum with the other etcd nodes in the etcd Cluster, then the RAMP triggers an auto-switchover.

In scenarios where the ETCD quorum is lost, although the communication is intact between the active and standby RAMPs, the OpenSAF controller stops all the RAMP processes on both the nodes to prevent a potential split-brain condition, resulting in both the nodes being moved to standby.

RAMP GR is supported for RAMP instances deployed in KVM, VMware, and OpenStack environments.

Prerequisites

- To enable the automatic switchover capability, ensure you have deployed the required three etcd VMs. Refer to [Setting Up an etcd Cluster](#).
- Two RAMP devices are up and running in the same environment with the same version.
- If the optional EdgeView (EV) service that enables managing SBC Edge devices is deployed, deploy it on both RAMP devices.
- For RAMP on KVM/VMware, the RAMP devices are running on separate host servers.
- The standby device is accessible from the active device, and vice versa.

If you have restored the database on an OpenStack deployment, password-less SSH from the active RAMP device to the standby RAMP device (and vice versa) is not possible until GR is configured.

- The same password is set for the `admin` and `insight` users on the active and standby devices.

The `insight` password is reset in the RAMP active device after restoring the database (with the password of the old database).

- If cron entries are created manually on the RAMP active device, you must also create the same cron entries on the standby device. In RAMP GR, cron entries are not copied and synchronized from active to standby, or vice versa.

To configure RAMP GR with automatic switchover, you must first create a redundancy template for the deployment and then run the GR setup script.

Generate a Redundancy Template

Use the script `RDbuild_config.sh` to generate a redundancy template for your GR deployment. This template is used to configure the deployment's redundancy parameters, including enabling the automatic switchover option.

1. Use the following command to generate a redundancy template. The script options are listed in the table below. Note that the example includes the "as" option to enable automatic switchover.

```
/etc/sonus/RDbuild_config.sh -o /opt/GRauto.conf -g gr:ipv4:as
```

Redundancy Template Script Parameters

Parameter	Description	Example	Optional (O) / Mandatory (M)?
-o	Name for the configuration file. Use this option along with -g.	<code>/etc/sonus/RDbuild_config.sh -o /opt/GRauto.conf -g gr:ipv4:as</code>	M
-g	Specify to generate a cluster configuration template. <code>RDbuild_config.sh -o <name for the template>.conf -g <the redundancy model>: <IP schema></code>	<code>/etc/sonus/RDbuild_config.sh -o /opt/GRauto.conf -g gr:ipv4:as</code>	M
<the redundancy model>	The redundancy model. Enter the following: ◦ gr for geographical redundancy	<code>/etc/sonus/RDbuild_config.sh -o GRauto.conf -g gr:ipv4:as</code>	M
<IP schema>	The IP schema. Enter the following: ◦ ipv4 for an IPv4 network ◦ ipv6 for an IPv6 network	<code>/etc/sonus/RDbuild_config.sh -o GRauto.conf -g gr:ipv4:as</code>	M

Parameter	Description	Example	Optional (O) / Mandatory (M)?
as	Option to enable automatic switchover	/etc/sonus/ RDbuidl_config.sh -o /opt/ GRauto.conf -g gr:ipv4:as	O
-h	List help topics.		O

2. Edit the generated template file to suit your deployment. Use the table below for more information on the parameters and values consistent with enabling automatic switchover.

Template File Parameters for GR Automatic Switchover

Parameter	Description	Value
Fixed Settings		
_primaryServer	The IP address of the node in which the cluster set up was initiated.	A valid IPv4/IPv6 address.
_clusterName	The name of the cluster.	Alphanumeric characters
_numSites	The number of sites in the cluster	2
_numNodes	The number of nodes in a site.	1
_pm_export_sync_to_standby	The flag to enable the PM export sync between active and standby nodes.	true or false
_totalNodes	The total number of nodes in the cluster.	2

Parameter	Description	Value
_ipschema	The IP address mode.	ipv4/ipv6
_site<site number>_name	The name for site <site number>.	Alphanumeric characters.
_auto_switchover	The flag to enable auto switchover.	yes
_arbitrator<number>_ip	The IP address of the arbitrator (etcd instance). For each of the 3 etcd instances.	A valid IPv4/IPv6 address.
_arbitrator<number>_port	The port number of the arbitrator (etcd instance). For each of the 3 etcd instances.	2379
_oss_info	The flag to configure Operations Support Systems (OSS) on RAMP.	no
Create Node (RAMP node information.)		
_node<node number>	The host name of the RAMP node <node number>.	Alphanumeric characters.
_node<node number>_id	The sequence number of the RAMP node <node number>.	1 or 2
_node<node number>_ip	The IP address of the RAMP node <node number>.	A valid IPv4/IPv6 address.
_node<node number>_site	The site name of the RAMP node <node number>.	Alphanumeric characters.

Configure RAMP GR Parameters

Use the following procedure to configure a RAMP GR deployment with automatic switchover enabled. Prior to running the procedure generate a redundancy template file that specifies to enable automatic switchover, as described in the previous section.

Run the GR configuration procedure on the RAMP device that you want as the source/active node for the GR deployment. It is not necessary to repeat the set up procedure on the target/standby device.

Start

1. On the RAMP device you want to establish as the source/active node in the GR deployment, log onto the CLI as the admin user.

2. Change to the `root` user.

```
sudo su -
```

3. Enter the following command, specifying the path and name for the redundancy template file generated for your GR deployment:

```
/etc/sonus/RDsetup.sh <absolute path to the redundancy template file>
```

An example specifying a redundancy template file, GRauto.conf, in the /opt directory:

```
/etc/sonus/RDsetup.sh /opt/GRauto.conf
```

An example output:

```
[16:17:41] Starting redundancy cluster setup .....  
[16:17:42]  
Building RD configuration locally .....  
Please enter Password of admin user for all nodes (press ENTER if not needed) ->  
admin
```

4. Enter the `admin` password.
The script completes setting up GR and the RAMP processes start shortly.
5. Log on to the activeRAMP node.
6. Change to the `insight` user to run a status check to verify that the system is healthy:

```
su - insight
```

7. Check the RAMP status:

```
/opt/sonus/ems/emsMgmt status
```

8. Log on to the CLI of the standby RAMP device as the `admin` user.
9. Change to the `insight` user:

```
sudo su - insight
```

10. Check the status on the RAMP standby node:

```
/opt/sonus/ems/emsMgmt status
```

If the configuration process is interrupted and you resume `RDsetup.sh`, the RAMP offers the following option:

```
Record showing the <script name> script was being executed and was not
completed.
Do you want to resume the operation from the previous point of failure (yes|
no)?.
```

Perform one of the following:

- Enter "yes" to resume the operation from the point of failure.
- Enter "no" to execute the script again. The RAMP shows the following message:

```
Do you want to proceed with a fresh new operation (yes|no)? ->
```

Perform one the following:

- Enter "yes" to execute the script.
- Enter "no" to terminate the session.

Setting Up an etcd Cluster

In this section:

- [Set up ETCD VMs on VMware](#)
 - [Create an ISO Configuration Drive for VMware](#)
 - [Create the etcd VMs Using the VMware GUI](#)
- [Set up the etcd VMs on KVM](#)
 - [Create an ISO Configuration Drive for KVM](#)
 - [Create the etcd VMs on a KVM Platform](#)
- [Set up etcd VMs on OpenStack](#)
- [Health Check etcd](#)

Related articles:

- [RAMP etcd System Requirements](#)
- [Configuring RAMP GR with Automatic Switchover Enabled](#)
- [Deployment Models](#)
- [RAMP Security Group Rules](#)
- [Configuring RAMP Redundancy](#)
- [Managing Redundancy](#)

For the purposes of monitoring a RAMP geographically redundant (GR) deployment to enable automatic switchover, three etcd VMs are required. Refer to [Configuring RAMP GR with Automatic Switchover Enabled](#) for information on how the etcd VMs are involved in the GR deployment.

You can instantiate these VMs on VMware, KVM, or OpenStack. You are not required to deploy the etcd VMs on the same platform as the RAMP instances.

Prerequisites

- Three free IPs are available to allocate to the etcd instances.
- The recommended configuration is 1 vCPU, 2GB of memory, and a minimum of 50GB of disk space. For more information, refer to [RAMP etcd System Requirements](#).
- Verify the network interfaces are connected and operable.
- Verify whether you have obtained the necessary installation files:
 - ISO configuration files
 - VMDK disk image files

Refer to [Download Files from Ribbon Support Portal](#) for information on using the portal.

Set up ETCD VMs on VMware

To set up ETCD on VMware-based VMs, first create an ISO configuration drive.

Create an ISO Configuration Drive for VMware

Complete the following procedure to set up an ISO configuration drive.

Start

1. Log on to the Ribbon Support portal. Download the `AppServices-configDrive.img` and the `AppServices-xx.xx.xxRxxx-xxxxx_vmCCS-x.x.x-xxxxx-xxx_xx.vmdk` files (refer to the release notes for the .vmdk file name).
Refer to [Download Files from Ribbon Support Portal](#) for information on using the portal.
2. Log on to a Linux server as the `root` user. On this server, create an `.iso` file from the provided template file (`AppServices-configDrive.img`) to use as a configuration drive for the VMs.
3. Create a temporary directory. In the following example the directory name is "etcd":

```
mkdir -p /tmp/etcd
```

4. Mount the image:

```
sudo mount AppServices-configDrive.img /tmp/etcd
```

5. Edit the cloud configuration. Refer to the following table for information on the parameters:

```
vim /tmp/etcd/user-data
```

Cloud Configuration Parameters

Parameters To Edit	Description	Example	Notes
hostname	Hostname of the VM in use	<code>hostname: "amm anetcd"</code>	

Parameters To Edit	Description	Example	Notes
fqdn	FQDN of the VM in use	fqdn: "ammanetc d.local"	
timezone	Choose the time zone	timezone: "Asia/ Kolkata"	
ntp	NTP server IP	servers: ["10.128.254.67"]	

Parameters To Edit	Description	Example	Notes
VnfName GatewayIpv4/ GatewayIpv6 ExternalIp	Name of the VNF as in "amman-ramp-geo-cluster" Gateway IP address of the etcd instance IP address of the etcd instance	# Ribbon vmCCS userdata: - content: { "VnfName": "amman-ramp-geo-cluster",	◦ Net{1,2,3}: Definition for the interface IF{1,2,3} ◦ Enabled : Indicates if the interface is enabled. Enabled is mandatory. You must set this to "true" or "false". ◦ GatewayIpv4: IPv4 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface ◦ GatewayIpv6: IPv6 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface. ◦ ExternalIp: External IP address for this interface ◦ Categories: List of category of traffic on this interface. By default, management is on net1, signaling and internal are on net2, and nothing is configured for net3. ◦ IsDefault: Indicates whether or not to assign the default route to this interface. Only one interface may have IsDefault=true . If false for all interfaces, the first interface with a gateway configured is assigned the default route. This parameter is not required if only one gateway was specified in the network-config file.

Parameters To Edit	Description	Example	Notes
		<pre> "Networks": { "Net1": { "Enabled": "True", "GatewayIpv4": "10.54.8.1", "GatewayIpv6": "", "ExternalIp": "10.54.8.166", "Categories": [], "IsDefault": "True" }, "Net2": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "ExternalIp": "", "Categories": [], "IsDefault": "" }, "Net3": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "ExternalIp": "", "Categories": [], "IsDefault": "" } }, </pre>	

Parameters To Edit	Description	Example	Notes
Etcd	Etcd configuration	<pre> "Etcd": { "ExistingEndpoints" : [], "PersistentDataPath" : "", "PersistentBackupPath" : "", "RootPassword" : "", "UserName" : "", "UserPassword" : "", "ClientCert" : "", "ClientKey" : "", "ClientCaCert" : "", "ServerCert" : "", "ServerKey" : "", "ServerCaCert" : "", "PeerCert" : "", "PeerKey" : "", "PeerCaCert" : "", "HeartbeatInterval" : "", "ElectionTimeout" : "", "BackupDiskMaxUse" : "", "BackupDiskKeepFree" : "", </pre>	◦ PersistentDataPath: Path to the persistent disk to use for Etcd data. The virtio number corresponds to the Etcd data volume ID provided in the deployment. ◦ RootPassword: The Etcd database password for the root user. If left blank, no authentication is enabled on the database. In a HA setup, the passwords must match on all the virtual machines. ◦ UserName: The name of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank. ◦ UserPassword: The password of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank. ◦ HeartbeatInterval: The interval (in ms) at which the leader notifies followers that it is still the leader. The recommended value to set is around the maximum of average round-trip time (RTT) between members, it is normally around 0.5-1.5x the round-trip time. If this field is left blank or omitted, the default value is 100 ms.

Parameters To Edit	Description	Example	Notes
		<pre>"BackupStartTime" : "", "BackupFullPeriod" : "0", "BackupRetention" : "" },</pre>	◦ ElectionTimeout: The duration (in ms) that a follower node performs without hearing a heartbeat before attempting to become the leader. The recommended value to set must be at least 10 times the RTT to account for a variance in the network. If this field is left blank or omitted, the default value is 1000 ms. ◦ BackupDiskMaxUse: The maximum percentage of the disk that allowed to be occupied by the Etcd backup files. The default value is 15. ◦ BackupDiskKeepFree: The percentage of disk that must be left free on the file system. The oldest backup files are deleted when this limit is reached. The default value is 30. ◦ BackupStartTime: The time of day when the scheduled backup starts. The format is in hh:mm±hh:mm. The first part of the format is the start time and second part is an offset (from UTC) to specify the time zone. If the time zone is not specified, then the local time zone of the virtual machine processing the request is used as the default time zone. The default value is 02:00.

Parameters To Edit	Description	Example	Notes
			◦ BackupFullPeriod : The interval at which a full backup of the etcd full is performed. This is expressed in the format of weeks and/or days, or hours. For example, 1w2d or 4h. Hours are not allowed to be provided with days or weeks. • The maximum allowed value for hours is 23h. • The minimum allowed value is 1h. • 0 means that no backup is performed. The default value is 1d. Note Set the BackupFullPeriod as 0 (Zero). ◦ BackupRetention : Specifies how long the backup files are retained before deleting the file(s). An empty value means that the backup files are retained for 7 days. This is expressed in the format of weeks, days and/or hours. For example, 1w24h or 2d.

Parameters To Edit	Description	Example	Notes
EtcdRegistries	IP addresses of any etcd instances created before	<pre>"VnfOperations": { "EtcdRegistries": [], "EtcdUserName": "admin", "EtcdUserPassword": "admin", "Salt": "mysalt@123"</pre>	VM communicate uses this function with the ETCD cluster for network function coordination, for example to register this VM for monitoring. Information on how to reach the ETCD cluster members and the options on how to fill this field are explained below: ◦ Recommended: Single entry pointing to an SRV FQDN that then points to all ETCD instances. This is recommended because SRV records can be updated with topology changes. ◦ Empty: This will cause the VM to always communicate to the local ETCD which has knowledge of the List of all planned members IPs.
VnfExistingInstances	IP addresses of any etcd instances created before	<pre>"VnfExistingInstances" : ["10.54.8.166","10.54.8.165"], "VnfReplaceInstance" : "", "UseMongoDB" : "", "UseEtcd" : "True", "UsePrometheus" : "", "UseAlertManager" : "";</pre>	While creating the first instance, "VnfExistingInstances" does not contain any value. While creating the second instance, "VnfExistingInstances" must contain the IP address of first etcd instance that was created. While creating the third instance, "VnfExistingInstances" must contain the IP addresses of the first and second etcd instances that were created.

6. Issue the following command to edit the network configuration:

```
vim /tmp/etcd/network-config
```

Edit the following parameters in the network-config file:

Parameters To Edit	Description	Example
addresses gateway4/gateway6	IP address to assign to this interface. The default gateway.	# DO NOT CHANGE version: 2 # List of network interfaces ethernets: # Network 1 eth0: addresses: # List of IP[v4,v6] addresses to assign to this interface - 10.54.48.60/23 # example: 10.20.30.5/24, fd00:10:6b50:5180::24/60 # Disable if not using IPv4 gateway4: "10.54.48.1" # Default IPv4 gateway – you can move it to another interface, if desired (example: default gateway on eth2) # Enable if using IPv6 # gateway6: "" # Default IPv6 gateway – you can move it to another interface, if desired (example: default gateway on eth2)

7. Run `genisoimage` command to create the `.iso` file:

```
genisoimage -o etcd.iso -V cidata -r /tmp/etcd
```

8. After creating the `.iso` file, issue the following commands to remove the temporary `etcd` directory:

```
sudo umount /tmp/etcd  
rm -rf /tmp/etcd
```

The ISO configuration is now complete.

9. Copy the `.iso` file created and the `AppServices-xx.xx.xxRxxx-xxxxxx_vmCCS-x.x.x-xxxxxx-xxx_xx.vmdk` files (refer to the release notes for the `.vmdk` file name) to the VMware host datastore location (`/vmfs/volumes/datastore1/etcdvnf`).

Create the etcd VMs Using the VMware GUI

Complete the following steps to instantiate the etcd VMs using the VMware GUI.

- Log on to the VMware ESXi GUI.
- Upload the VMDK and ISO installation files to the VMware server using the VMware ESXi GUI:
 - In the left navigation menu, select **Storage**.

- b. Under **Storage**, select a datastore device to which you want to upload.
- c. Select **Datastore browser**.
- d. Within the datastore, select an existing directory where you want to store the original images, or click **Create directory** to create a new directory for this purpose. **Example directory name:**
`etcdvnf-orig`.
- e. In the target directory, select **Upload** and then navigate to one of the installation files and upload it. Select **Upload** again and repeat the process to locate and upload each VMDK and ISO file until you have uploaded all of the installation files.
- f. Check the Datastore browser status or check the VMware GUI's "Recent Tasks" pane to ensure that all of the uploads are completed before continuing.

The uploaded VMDK files are in a sparse format. Sparse disk images cannot be used directly to launch a VM. These files must be converted to a flat format. The process of copying the files, as described in the following step, automatically converts the files to the flat format that is required to launch a VM.

3. Create a copy of the appropriate VMDK image file (AppServices) for each VM you plan to deploy.

Copies are essential because, during the VM creation process, the VMDK image file is transformed into a disk image. This means you cannot reuse the same file to create another VM instance. To launch multiple VM instances, you need to make a copy of the original VMDK image file for each instance. Each time you create a copy, the VMDK file is automatically converted into a flat VMDK file, which can then be used to launch a VM.

To copy a VMDK image file:

- a. In the **Datastore browser**, select an original VMDK file that was uploaded and select **Copy**.
- b. Select an existing folder that you want to hold the active VM disk images or click **Create directory** to create a new directory for this purpose. **Example directory name:** `etcdvnf`.
- c. Name the image file copies appropriately according to the type of VM they will launch. Ribbon recommends to include the version in the name to avoid confusion during upgrade.
Examples: `vmwappdb1_23.02.00R000.vmdk`, `vmwappdb2_23.02.00R000.vmdk`.
- d. Repeat the previous steps to copy an original VMDK image file for each VM that you plan to launch.

4. Create the first VM.

These instructions apply to all the VMs: initially to the first Services VM, and then to the second and third Services VMs, respectively.

For CPU, memory (RAM), Hard Disk and Host OS requirements of each VM, refer to [RAMP etcd System Requirements](#).

- a. Create the new VM.
 From the VMware GUI home menu, use the menus to create a new VM.
 - i. Select *Virtual Machines -> Create / Register VM -> Create a new virtual machine*.
 - ii. Click **Next** to continue.
 - iii. In the **Select a name and guest OS** menu:
 1. Provide the host name for the VM.
Example host name for the first Services VM: `vmwappdb1`

2. Select the Operating System (OS).
Example: Compatibility ESXi 6.7 virtual machine, Guest OS Family Linux, Guest OS Version **Red Hat Enterprise Linux 8 (64-bit)**.
 - iv. Click **Next** to continue.
 - v. In the **Select storage** menu:
 1. If the Standard and Persistent Memory options appear, select **Standard** for the storage type.
 2. Choose the appropriate datastore for the VM's configuration files and virtual disks.
Example datastore name: datastore1, Capacity: 500 GB, Free: 460 GB, Type: VMFS6, Thin provisioning: Supported, Access: Single
 - vi. Click **Next** to continue.
- b. Customize the new VM.
- In the **Customize settings** menu, configure the VM hardware.
- i. Select the **VM Options** tab.
 1. Click **Boot options** from the list.
 2. Select **BIOS** for Firmware.
 - ii. Select the **Virtual Hardware** tab.
 - iii. Configure the VM CPU and memory.
Example configurations:
 1. Select **1 CPU and 2 GB RAM** for a Services VM.
 - iv. Set up the VMDK (Virtual Machine Disk) hard drive.
 1. Delete the default hard disk (Hard disk 1) by selecting the "X" next to it.
 2. Select **Add hard disk**.
 3. In the pop-up window select **Existing hard disk**.
 4. In the **Datastore browser** window, browse the datastore folder and select the file corresponding to the appropriate VMDK file you created earlier.
 - a. Example file name if creating a Services VM: vmwappdb1.vmdk (or vmwappdb2.vmdk or vmwappdb3.vmdk)
 5. Click **Select** to continue.
 6. Change the **Controller location** (or "Virtual Device Node") and "Virtual Device Node unit" to **IDE controller 0** and **Master**.
 7. Click the expand/contract triangle of the **New Hard disk** list to contract the list and make the rest of the **Customize settings** visible.
 - v. Set up the ISO configuration drive.
- Warning**

Even after initial installation, the configuration drive must remain mounted.
1. On the CD/DVD Drive change the drop down to **Datastore ISO file**.
 2. In the **Datastore browser** window, browse the datastore folder and select the file corresponding to the appropriate ISO file you transferred earlier.
 - a. Example file name if creating a Services VM:
vmwappdb1.iso (or vmwappdb2.iso or vmwappdb3.iso if creating the second or third Services VM)
 3. Click **Select** to continue.
- vi. **Configure Networking.**
Select the appropriate network.
- c. Finish creating the new VM and power it on.
- i. Click **Next** in the **Customize settings** menu to continue.

- ii. In the **Ready to complete** menu, review the settings you have selected.
- iii. Click **Finish** to complete the creation of the VM.
- iv. Power on (activate) the VM.
In the list of Virtual Machines, right-click the VM you just created.
Select *Power* -> *Power on*.
- v. Verify the services that are running on the VM. After about ten minutes, run the `vmccs-status` command from the SSH login to verify all services are running on the VM.

Note

Once all services are up and running, you can start the next VM.

Set up the etcd VMs on KVM

To set up ETCD on KVM-based VMs, first create an ISO configuration drive.

Create an ISO Configuration Drive for KVM

Complete the following procedure to set up an ISO configuration drive.

Start

1. Log on to the Ribbon Support portal. Download the `AppServices-configDrive.img` and the `AppServices-22.07.00R000-B3500_vmCCS-1.4.1-B2297-x86_64.qcow2` files. Refer to [Download Files from Ribbon Support Portal](#) for information on using the portal.
2. Log onto a Linux server as the `root` user. On this server, create an `.iso` file from the provided template file (`AppServices-configDrive.img`) to use as a configuration drive for the VMs.
3. Create a temporary directory. In the following example the directory name is "etcd":

```
mkdir -p /tmp/etcd
```

4. Mount the image.

```
sudo mount AppServices-configDrive.img /tmp/etcd
```

5. Issue the following command to edit the cloud configuration. Refer to the following table for information on the parameters:

```
vim /tmp/etcd/user-data
```

Cloud Configuration Parameters

Parameters To Edit	Description	Example	Note
hostname	Hostname of the VM in use	hostname: "amma netcd"	

Parameters To Edit	Description	Example	Note
fqdn	FQDN of the VM in use	fqdn: " ammanetc d .local"	
timezone	Choose the time zone	timezone: "Asia/ Kolkata"	
ntp	NTP server IP	servers: ["10.128.254.67"]	

Parameters To Edit	Description	Example	Note
VnfName GatewayIpv4/ GatewayIpv6 Externallp	hostname: ammanetcd1 VnfName: amman- ramp-geo-cluster Gateway IP address of the etcd instance Externally visible IP address of the ETCD instance.	# Ribbon vmCCS userdata: - content: { "VnfName": "amman-ramp-geo- cluster",	◦ Net{1,2,3}: Definition for the interface IF{1,2,3} ◦ Enabled : Indicates if the interface is enabled. Enabled is mandatory. You must set it to "true" or "false". ◦ GatewayIpv4: IPv4 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface ◦ GatewayIpv6: IPv6 gateway address for this interface, used to create a default route for egress packets with the source IP assigned to this interface ◦ ExternalIp: The IP used to access the interface from an external source may differ. For instance, if the virtual machine (VM) is behind a NAT, like when using a floating IP in an OpenStack environment, the externally visible IP will not match the internal IP configured on the VM's interface. This is necessary to ensure that we present the correct external IP to the outside world. ◦ Categories: List of category of traffic on this interface. By default, management is on net1, signaling and internal are on net2, and nothing is configured for net3.

Parameters To Edit	Description	Example	Note
		<pre> "Networks": { "Net1": { "Enabled": "True", "GatewayIpv4": "", "GatewayIpv6": "fd00:10:6b50:40c0: :1", "Externallp": "fd00:10:6b50:40c0: :24", "Categories": [], "IsDefault": "True" }, "Net2": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "Externallp": "", "Categories": [], "IsDefault": "" }, "Net3": { "Enabled": "False", "GatewayIpv4": "", "GatewayIpv6": "", "Externallp": "", "Categories": [], "IsDefault": "" } } </pre>	◦ IsDefault: Indicates whether or not to assign the default route to this interface. Only one interface may have IsDefault=true. If false for all interfaces, the first interface with a gateway configured is assigned the default route. This parameter is not required if only one gateway was specified in the network-config file.

Parameters To Edit	Description	Example	Note
Etcd	Etcd configuration	<pre> "Etcd": { "ExistingEndpoints" : [], "PersistentDataPath" : "", "PersistentBackupPath" : "", "RootPassword" : "", "UserName" : "", "UserPassword" : "", "ClientCert" : "", "ClientKey" : "", "ClientCaCert" : "", "ServerCert" : "", "ServerKey" : "", "ServerCaCert" : "", "PeerCert" : "", "PeerKey" : "", "PeerCaCert" : "", "HeartbeatInterval" : "", "ElectionTimeout" : "", "BackupDiskMaxUse" : "", "BackupDiskKeepFree" : "" </pre>	◦ PersistentDataPath: Path to the persistent disk to use for Etcd data. The virtio number corresponds to the Etcd data volume ID provided in the deployment. ◦ RootPassword: The Etcd database password for the root user. If left blank, no authentication is enabled on the database. In a HA setup, the passwords must match on all the virtual machines. ◦ UserName: The name of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank. ◦ UserPassword: The password of a user to create in the Etcd database. This field is ignored if the RootPassword is empty. No user is created if this field is left blank. ◦ HeartbeatInterval: The interval (in ms) at which the leader notifies followers that it is still the leader. The recommended value to set is around the maximum of average round-trip time (RTT) between members, it is normally around 0.5-1.5x the round-trip time. If this field is left blank or omitted, the default value is 100 ms.

Parameters To Edit	Description	Example	Note
		<pre>"BackupStartTime" : "", "BackupFullPeriod" : "0", "BackupRetention" : "" },</pre>	◦ ElectionTimeout: The duration (in ms) that a follower node performs without hearing a heartbeat before attempting to become the leader. The recommended value to set must be at least 10 times the RTT to account for a variance in the network. If this field is left blank or omitted, the default value is 1000 ms. ◦ BackupDiskMaxUse: The maximum percentage of the disk that allowed to be occupied by the Etcd backup files. The default value is 15. ◦ BackupDiskKeepFree: The percentage of disk that must be left free on the file system. The oldest backup files are deleted when this limit is reached. The default value is 30. ◦ BackupStartTime: The time of day when the scheduled backup starts. The format is in hh:mm±hh:mm. The first part of the format is the start time and second part is an offset (from UTC) to specify the time zone. If the time zone is not specified, then the local time zone of the virtual machine processing the request is used as the default time zone. The default value is 02:00.

Parameters To Edit	Description	Example	Note
			◦ BackupFullPeriod : The interval at which a full backup of the Etcd full is performed. This is expressed in the format of weeks and/or days, or hours. For example, 1w2d or 4h. Hours are not allowed to be provided with days or weeks. • The maximum allowed value for hours is 23h. • The minimum allowed value is 1h. • 0 means that no backup is performed. The default value is 1d. NOTE: Set the BackupFullPeriod as 0 (Zero). ◦ BackupRetention : Specifies how long the backup files are retained before deleting the file(s). An empty value means that the backup files are retained for 7 days. This is expressed in the format of weeks, days and/or hours. For example, 1w24h or 2d.

Parameters To Edit	Description	Example	Note
EtcdRegistries	Information to connect to the ETCD cluster	<pre>"VnfOperations": { "EtcdRegistries": [], "EtcdUserName": "admin", "EtcdUserPassword": "admin", "Salt": "mysalt@123"</pre>	VM communicate uses this function with the ETCD cluster for network function coordination, for example to register this VM for monitoring. Information on how to reach the ETCD cluster members and the options on how to fill this field are explained below: ◦ Recommended: Single entry pointing to an SRV FQDN that then points to all ETCD instances. This is recommended because SRV records can be updated with topology changes. ◦ Empty: This will cause the VM to always communicate to the local ETCD which has knowledge of the List of all planned members IPs.
VnfExistingInstances	IP addresses of any etcd instances created before	<pre>"VnfExistingInstances": ["10.54.8.166","10.54.8.165"], "VnfReplaceInstance" : "", "UseMongoDB" : "", "UseEtcd" : "True", "UsePrometheus" : "True", "UseAlertManager" : "True",</pre>	While creating the first instance, "VnfExistingInstances" does not contain any value. While creating the second instance, "VnfExistingInstances" must contain the IP address of first etcd instance that was created. While creating the third instance, "VnfExistingInstances" must contain the IP addresses of the first and second etcd instances that were created.

Parameters To Edit	Description	Example	Note
Prometheus	Prometheus configuration	"Prometheus": { "PersistentDataPath" " : "", "MaxDiskUsage" : "40" }	Prometheus configuration Fields: ◦ PersistentDataPath: Path to the persistent disk to use for Prometheus and AlertManager data. The virtio number corresponds to the Prometheus data volume ID provided in the deployment. ◦ MaxDiskUsage: Maximum disk usage allowed by Prometheus data in percent of the total disk size.

Example etcd userdata:

```
#cloud-config

# Hostname to use for this VM
hostname: "ammanetcd"

# FQDN to use for this VM, usually just <hostname>.local
fqdn: "ammanetcd.local"

# DO NOT CHANGE
preserve_hostname: false

# DO NOT CHANGE
manage_etc_hosts: true

# List of groups to create on this VM
groups:
  # User part of this group can read backup files
  - backup_group # This group name is used by ansible during the VM initial
  configuration

# List of users to create/update on this VM
users:
  # Recommended user for systems administrators
  - name: root
    plain_text_passwd: "Sonus@123"
    lock_passwd: false

  - name: sysadm
    plain_text_passwd: "shipped!!"
```



```

lock_passwd: false
ssh_authorized_keys:
  - "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAqJX+iihNx0PZNHwBXbEogknmUH2xvupn8/
bcx9YmAT7RcVsj4ICMIGic1yAJjhdRWgTRwpGqBKzfTUVanBZS232aBETPMGZHGtdpjpFdUMGHiYU4niwm
mwGzp84mnyZoqwh5pGau9ZTJL2IUjyh0t7a/s2RXHu88HHC4+SduD5fWiU0GL0bc8re2lXdkUIlk/
Sg430GNqHW68SnZI7yPWZJbv9z3+6qN2oxvBqd/
eb9RbQQzoupSci0BFBkYhUiRFbNQZAcTF7+4XFkraSnBLtYckN+EPDJv4G/
Uk9bi65320g5SQPFoXEzenk2STLJq0tiCcMeX04fIw0bhCOSgQ== ssequeira@ptbats"

# Timezone for this VM (format: tz database, e.g. "America/New_York")
timezone: "Asia/Kolkata"

# List of NTP servers to use on this VM
ntp:
  servers: ["10.128.254.67"]
  ntp_client: chrony # DO NOT CHANGE
  config:
    service_name: chronyd # DO NOT CHANGE

# Files that will be written to disk
write_files:
  # DO NOT CHANGE
  - content: |
      {
        "TemplateName": "heat_template.yaml"
      }
    path: /opt/rbbsn/userData.json
    owner: root:root
    permissions: '0600'

# Ribbon vmCCS userdata: fill in all fields according to user guide
- content: |
    {
      "VnfName": "amman-ramp-geo-cluster",

      "Networks": {
        "Net1": {
          "Enabled": "True",
          "GatewayIpv4": "",
          "GatewayIpv6": "",
          "ExternalIp": "172.19.52.209",
          "Categories": [],
          "IsDefault": "true"
        },
        "Net2": {
          "Enabled": "False",
          "GatewayIpv4": "",
          "GatewayIpv6": "",
          "ExternalIp": "",
          "Categories": [],
          "IsDefault": "false"
        }
      }
    }

```

```

    },
    "Net3": {
      "Enabled": "False",
      "GatewayIpv4": "",
      "GatewayIpv6": "",
      "ExternalIp": "",
      "Categories": [],
      "IsDefault": "false"
    }
  },
  "VnfOperations": {
    "EtcdRegistries": [],
    "EtcdUserName": "",
    "EtcdUserPassword": "",
    "Salt": ""
  },
  "ServiceDiscovery": {
    "RegistryType": "dns",
    "Registries": []
  },
  "Logging": {
    "Elasticsearch": {
      "Hosts": [{
        "Addr": "",
        "Port": "",
        "HttpUser": "",
        "HttpPasswd": "",
        "TlsEnable": "Off",
        "TlsVerify": "On",
        "RecordTypeFilters": ["tdr","log"]
      }],
      "Index": ""
    },
    "Syslog": {
      "Hosts": [{
        "Addr": "10.54.21.201",
        "Port": "514",
        "RecordTypeFilters": ["tdr","log"]
      }],
      "Protocol": "udp",
      "CACert": ""
    },
    "Fluent": {
      "Hosts": [{
        "Addr": "",
        "Port": "",
        "RecordTypeFilters": ["tdr","log"]
      }],
    }
  },
},

```

```

        "Metrics": {
            "Export": "True"
        }
    }
    path: /etc/rbbn/podman/userdata.json
    owner: root:root
    permissions: '0600'

# Ribbon AppServices userdata: fill in all fields according to user guide
- content: |
    {
        "VnfExistingInstances" : ["172.19.52.139","172.19.52.129"],
        "VnfReplaceInstance"   : "",
        "UseMongoDB"           : "False",
        "UseEtcd"               : "True",
        "UsePrometheus"         : "True",
        "UseAlertManager"       : "True",

        "MongoDB": {
            "PersistentDataPath"      : "",
            "PersistentBackupPath"    : "",
            "AuthKey"                 : "",
            "AdminPassword"           : "",
            "UserName"                : "",
            "UserPassword"            : "",
            "BackupDiskMaxUse"        : "15",
            "BackupDiskKeepFree"      : "30",
            "BackupStartTime"         : "02:00",
            "BackupFullPeriod"        : "1d",
            "BackupDifferentialPeriod" : "4h",
            "BackupRetention"         : ""
        },

        "Etcd": {
            "ExistingEndpoints"       : [],
            "PersistentDataPath"      : "",
            "PersistentBackupPath"    : "",
            "RootPassword"            : "",
            "UserName"                : "",
            "UserPassword"            : "",
            "ClientCert"              : "",
            "ClientKey"               : "",
            "ClientCaCert"            : "",
            "ServerCert"              : "",
            "ServerKey"               : "",
            "ServerCaCert"            : "",
            "PeerCert"                : "",
            "PeerKey"                 : "",
            "PeerCaCert"              : "",
            "HeartbeatInterval"       : "100",
            "ElectionTimeout"         : "1000",
            "BackupDiskMaxUse"        : "15",

```

```

        "BackupDiskKeepFree"    : "30",
        "BackupStartTime"       : "02:00",
        "BackupFullPeriod"      : "0",
        "BackupRetention"       : ""
    },

    "Prometheus": {
        "PersistentDataPath"    : "",
        "MaxDiskUsage"          : "40"
    }
}
path: /etc/rbbn/appservices/userdata.json
owner: root:root
permissions: '0600'

# DO NOT CHANGE
runcmd:
  # Launch main vmCCS playbook (downstream plays are launched by this playbook)
  - ansible-playbook /etc/rbbn/podman/configure.yml

```

6. Issue the following command to edit the network configuration:

```
vim /tmp/etcd/network-config
```

Edit the following parameters in the network-config file:

Parameters To Edit	Description	Example
addresses	IP address to assign to this interface.	# DO NOT CHANGE version: 2
gateway4/ gateway6	The default IP gateway.	# List of network interfaces ethernets: # Network 1 eth0: addresses: # List of IP[v4,v6] addresses to assign to this interface - 10.54.48.60/23 # example: 10.20.30.5/24, fd00:10:6b50:5180::24/60 # Disable if not using IPv4 gateway4: "10.54.48.1" # Default IPv4 gateway – can move it to another interface, if desired (example: default gateway on eth2) # Enable if using IPv6 # gateway6: "" # Default IPv6 gateway – you can move it to another interface if desired (example: default gateway on eth2)

7. Issue the `genisoimage` command to create the ISO file:

```
genisoimage -o etcd.iso -V cidata -r /tmp/etcd
```

8. After creating the ISO file, issue the following commands to remove the temporary etcd directory:

```
sudo umount /tmp/etcd
rm -rf /tmp/etcd
```

The ISO configuration is now complete.

9. Copy the `.iso` file created and the `AppServices-22.07.00R000-B3500_vmCCS-1.4.1-B2297-x86_64.qcow2` to the KVM host.

Create the etcd VMs on a KVM Platform

Complete the following steps to instantiate the etcd VMs on a KVM platform.

Start

1. Install the VNF using `virt-install`.

In the following example command:

`--network` assumes that a bridge called `br0` is the VNF's network interface. If you choose to deploy with two network interfaces, add another `--network` statement with the bridge for the second interface. The order of `--network` is the same as the order of interfaces in the VM (`eth0`, `eth1`, ...).

```
export VNF_NAME=ammanetcd # Replace with your desired VM name

sudo virt-install \
  --name $VNF_NAME \
  --memory 2048 \
  --disk /var/lib/libvirt/images/AppServices-22.07.00R000-B3500_vmCCS-1.4.1-B2297-x86_64.qcow2,device=disk,bus=virtio \
  --disk /var/lib/libvirt/images/etcd.iso,device=disk,bus=virtio,readonly=on \
  --os-type linux \
  --os-variant rhel8.2 \
  --graphics none \
  --network bridge=br0,model=virtio \
  --import
```

To validate that services are running once the VM is ready, check the status of `appservices` using the following command as `sysadm` user.

```
$ vmccs-status
```

Example vmccs-status output:

```

$ vmccs-status
Validating backup-manager services status...
    backup-manager: active (running)
backup-manager is active

Validating Etcd services status...
    etcd: active (running)
Etcd is active

Validating Fluentbit services status...
    td-agent-bit: active (running)
    fluent-sd: active (running)
    fluent-sd-watch: active (running)
Fluentbit is active

Validating nginx services status...
    nginx: active (running)
    nginx-exporter: active (running)
nginx is active

Validating Node Exporter services status...
    node-exporter: active (running)
Node Exporter is active

Validating Prometheus services status...
    prometheus: active (running)
    prometheus-autoconfig: active (running)
    alertmanager: active (running)
    alertmanager-watch: active (running)
Prometheus is active

Validating SDR services status...
    sdr: active (running)
SDR is active

Validating VNF Operations services status...
    vnf-operations: active (running)
VNF Operations is active

All required vmCCS services are active.

```

Network **interface** roles

```

.-----+-----+-----+-----+
| Default Gateway | Management | Internal  | Signaling |
.-----+-----+-----+-----+
|      eth0      |      eth0  |      eth0 |      eth0  |
.-----+-----+-----+-----+

```

Set up etcd VMs on OpenStack

Complete the following steps to instantiate VMs on OpenStack on which you will run etcd.

Start

1. Log on to the Ribbon Support portal. Download the Heat template file (heat_template.yml) and image file (AppServices-22.12.00R000-B4256_vmCCS-1.5.3-x86_64.qcow2). Refer to [Download Files from Ribbon Support Portal](#) for information on using the portal.
2. Create or re-use an existing flavor that specifies the recommended configuration (1 vCPU, 2GB of memory, 50GB of disk space). Refer to [Create an OpenStack Flavor](#).
3. Create a security group that defines "allow" rules for the following ingress and egress traffic. Refer to [Create a Security Group](#).

Port	Description
2381	etcd Prometheus exporter
9013	Nginx Prometheus exporter
9100	Prometheus node exporter (metrics)
9292	Backup-manager Prometheus exporter
9090	Prometheus
9093	Prometheus AlertManager client
9801	Service Discovery Representative (SDR) Prometheus exporter
9802	nf-operations exporter
9803	vnf-operations exporter
24231	Fluentbit Prometheus exporter
9094	Prometheus AlertManager cluster communication
2379	etcd client requests
2380	etcd peer communication

4. Configure an external network for your deployment. Refer to [Create an External Network](#).

Name	Description	Default
ext_net1	Public network with floating IP addresses for network 1. Used to allocate a floating IP to the instance.	EXT_OAM_0_STATIC

5. Create a ETCD image on the Glance image server using the qcow2 image file you downloaded. Refer to [Create a Glance Image](#).
6. Use the OpenStack GUI to launch the etcd instance. On the **Launch Stack** window, use the following table to edit the following configurations, as needed, for your environment.

Parameter	Description	Mandatory	Example
image	Image to use for the etcd VM, use the image uploaded in step 5	Yes	AppServices-22.12.00A000-B4225_vmCCS-1.6.0-alpha-B2575-x86_64.qcow2
flavor	OpenStack flavour to use, use the flavour created at step 2	Yes	46fd3493-108e-456d-9c47-66a1ea95d699
security group	Security group to use for the VM, use the security group create at step 3	Yes	default
authorized key	SSH public keys authorized to connect to this VNF.	Yes	
availability zone	Network availability zone for this VNF.	No	
management interface hostname	Hostname to use for management interface.	No	ammanetcd
management interface domain name	Domain name to use for management interface.	No	local
user root password	Password for the root user of the VNF instance.	No	Sonus@123
user sysadm password	Password for the <code>sysadm</code> user of the VNF instance. (<code>sysadm</code> is the administrative account)	Yes	Sonus@123

Parameter	Description	Mandatory	Example
Etcd registries	VM communicate uses this function with the etcd cluster for network function coordination, for example to register this VM for monitoring. Information on how to reach the etcd cluster members and the options on how to fill this field are explained below: ◦ Recommended: Single entry pointing to an SRV FQDN that then points to all etcd instances. This is recommended because SRV records can be updated with topology changes. ◦ Empty: This will cause the VM to always communicate to the local etcd which has knowledge of the List of all planned members IPs.	No	
Existing VNF instances	IP addresses of any etcd instances created before.	Yes	fd00:10:6b50:61b0::4c7,fd00:10:6b50:61b0::1bc
Etcd username	Name of an etcd user with read/write permissions to all keys related to VNF operations.	No	
Etcd password	Password of for the etcd user with read/write permissions to all keys related to VNF operations.	No	
Salt	Salt value for cryptography operations done during VNF operations. Ensure it is the same for all VMs of a deployment. Ribbon recommends making it unique per deployment.	No	
Use Etcd	Provide etcd as a service.	Yes	true
Use_prometheus	Provide Prometheus as a service.	Yes	true

Parameter	Description	Mandatory	Example
Use_alertmanager	Provide Prometheus Alertmanager as a service.	Yes	true
Use_mongo	Provide a MongoDB server as a service.	Yes	False
etcd_data_volume_id	Identifier of the Cinder volume to use for etcd data.	No	
etcd_backup_volume_id	Identifier of the Cinder volume to use for etcd backup.	No	
etcd_root_password	Password for the etcd root user. This user has all access to etcd including creation of users, policies, removing kes store etc.	No	
etcd_user_name	Username for a etcd user. This user has read/write permission on path with same name.	No	
etcd_user_password	Password for the etcd user.	No	
etcd_client_cert	etcd GRPC client certificate. Used for init and etcdctl commands.	No	
etcd_client_key	etcd GRPC client private key. Used for init and etcdctl commands.	No	
etcd_client_ca_cert	etcd GRPC client CA certificate. Used for init and etcdctl commands.	No	
etcd_server_cert	etcd GRPC server certificate. Used for grpc server.	No	
etcd_server_key	etcd GRPC server private key. Used for grpc server.	No	
etcd_server_ca_cert	etcd GRPC server CA certificate. Used for grpc server.	No	
etcd_peer_cert	etcd GRPC peer certificate. Used for clustering.	No	

Parameter	Description	Mandatory	Example
etcd_peer_key	etcd GRPC peer private key. Used for clustering.	No	
etcd_peer_ca_cert	etcd GRPC peer CA certificate. Used for clustering.	No	
etcd_heartbeat_interval	Interval in ms at which the leader will notify followers that it is still the leader.	No	
etcd_election_timeout	Describes how long in ms a follower node will go for without hearing a heartbeat before attempting to become leader itself.	No	
etcd_backup_disk_max_use	Maximum percentage of the disk that may be occupied by etcd backup files.	No	
etcd_backup_disk_keep_free	Percentage of disk that must be left free on the file system. The oldest backup files will be deleted when this limit is reached.	No	
etcd_backup_start_time	Time of day when backup schedule starts in hh:mm+hh:mm or hh:mm-hh:mm format. First part of the format is the start time and second part is an offset (from UTC) for specifying the time zone. If the time zone is not specified, local time zone of the VM processing the request will be used as the default time zone.	No	
etcd_backup_full_period	Interval at which the etcd full backups are performed. Expressed in weeks and/or days, or hours format, e.g. 1w2d or 4h. Hours cannot be provided with days or weeks. Maximum value for hour is 23h. 0 means that no backup is performed.	No	

Parameter	Description	Mandatory	Example
etcd_backup_retention	Time specifies how long to wait before deleting the file(s). Empty value means that we keep the files for 7 days. It is expressed in weeks, days and/or hours format, e.g. 1w24h or 2d.	No	
prometheus_data_volume_id	Identifier of the Cinder volume to use for Prometheus and/or AlertManager data.	No	
prometheus_max_disk_usage_in_percent	Maximum disk usage allowed by Prometheus data in percent of the total disk size.	No	
DNS nameserver(s)	Comma-separated list of DNS nameservers to use in the private subnet.	No	fd00:10:6b50:61c0::4d1,fd00:10:6b50:61c0::4d2
DNS search domains	Comma-separated list of DNS search domains to use in the private subnet.	No	rbbn.com
NTP server(s)	Comma-separated list of time servers to use for clock synchronization.	No	fd00:10:6b50:61c0::4d3
NTP time zone	Time zone used for clock synchronization.	No	America/New_York
elasticsearch_host_addr	Remote Elasticsearch node's hostname or IP address. Used for log aggregation.	No	
elasticsearch_host_port	Remote Elasticsearch node port. Used for log aggregation.	No	
elasticsearch_index	Index name to use for Elasticsearch logging destination. Used for log aggregation.	No	
elasticsearch_http_user	Username credential for X-Pack access.	No	

Parameter	Description	Mandatory	Example
elasticsearch_http_password	Password for user defined in HTTP_User.	No	
elasticsearch_tls_enabled	Enable or disable TLS support.	Yes	Off
elasticsearch_tls_verify	Force certificate validation.	Yes	On
elasticsearch_record_type_filters	Comma-separated list of record type filter(s) to use for elasticsearch (tdr, log)	Yes	tdr, log
syslog_host_addr	Remote syslog node's hostname or IP address. Used for log aggregation.	Yes	10.54.21.201
syslog_host_port	Remote syslog node's port. Used for log aggregation.	Yes	514
syslog_protocol	Remote syslog node's transport protocol. Used for log aggregation.	Yes	"udp", "tcp", "tls"
syslog_record_type_filters	Comma-separated list of record type filter(s) to use for syslog (tdr, log)	Yes	tdr,log
syslog_ca_cert	Remote syslog node's CA certificate. Used for sending logs over TLS (protocol set to 'tls'). Line breaks must be converted to '\n' - see user guide.	No	
fluent_host_addr	FluentD/Fluent Bit aggregator node hostname or IP address. Used for log aggregation.	No	
fluent_host_port	FluentD/Fluent Bit aggregator node port. Used for log aggregation.	No	
fluent_record_type_filters	Comma-separated list of record type filter(s) to use for FluentD/Fluent Bit aggregator node (tdr, log).	Yes	

Parameter	Description	Mandatory	Example
ext_net1	Network 1 used to allocate an IP to the instance.	Yes	EXT_OAM_0_STATIC
use_net2	If true, add a second network interface.	Yes	False
ext_net2	Network 2 used to allocate an IP to the instance.	No	
use_net3	If true, add a third network interface.	Yes	False
ext_net3	Network 3 used to allocate an IP to the instance.	Yes	
default_net	Network on which default gateway is defined. This determines the interface which is assigned the 0.0.0.0/0 route in the server.	Yes	
management_net	Network used for configuration, management and metrics traffic. If network 2 or 3 are specified, they must be enabled.	Yes	1
signaling_net	Network used for signaling traffic. If network 2 or 3 are specified, they must be enabled.	Yes	2
internal_net	Network used for database & application-internal traffic. If network 2 or 3 are specified, they must be enabled.	Yes	2
routes_net1	Comma-delimited list of destination subnets for which traffic should be sent through eth0 (network 1). These routes should align with the ingress networks configured above. Multiple routes may be specified as a comma-delimited list.	No	

Parameter	Description	Mandatory	Example
routes_net2	Comma-delimited list of destination subnets for which traffic should be sent through eth1 (network 2). These routes should align with the ingress networks configured above. Multiple routes may be specified as a comma-delimited list.	No	
routes_net3	Comma-delimited list of destination subnets for which traffic should be sent through eth2 (network 3). These routes should align with the ingress networks configured above. Multiple routes may be specified as a comma-delimited list.	No	
service_registries	Comma-separated list of service registry servers to use for service discovery.	No	
dns_nameservers	Comma-separated list of DNS nameservers to use in private subnet.	No	
dns_search	Comma-separated list of DNS search domains to use in private subnet.	No	
ntp_servers	Comma-separated list of time servers to use for clock synchronization.	Yes	10.128.254.67
time_zone	Time zone used for clock synchronization. Format: time zone database, e.g. 'America/New_York'	Yes	Asia/Kolkata
vnf_instances	Comma-separated list of existing VNF instance(s) IP address. The internal interface IPs of the previously instantiated instances in the AppServices cluster should be applied here.	No	

Parameter	Description	Mandatory	Example
vnf_replace	Existing VNF instance IP address to replace. This new instance will replace the instance specified here.	No	
use_etcd	Provide etcd as a service.	True	
use_prometheus	Provide Prometheus as a service.	True	
use_alertmanager	Provide Prometheus Alertmanager as a service.	True	
backup_username	Defines a user that can access and retrieve the DB backup files.	Yes	backup_user
backup_user_password	Password for the backup user of the VNF instance. If left blank, user will not be created.	No	
backup_user_key	SSH public key authorized to connect to the backup user account. Use this parameter with caution in production settings.	No	
mongo_data_volume_id	Identifier of the Cinder volume to use for MongoDB data.	No	
mongo_backup_volume_id	Identifier of the Cinder volume to use for MongoDB backup.	No	
mongo_authkey	Authentication key used to authenticate each MongoDB instances together. Only required when using password authentication.	No	MongoDB auth key must be between 6 and 1024 characters and use base64 characters only.
mongo_admin_password	Password for the MongoDB admin user. This user has read/write permissions in all databases. If this is left empty, MongoDB will be configured without authentication.	No	

Parameter	Description	Mandatory	Example
mongo_user_name	Username for a MongoDB user. This user has read/write permissions on a database of the same name.	No	
mongo_user_password	Password for the MongoDB user. Allowed special characters are: ! [*._]~+-(){}^=/@#?;&`<>	No	
mongo_backup_disk_max_use	Maximum percentage of the disk that may be occupied by MongoDB backup files.	Yes	15
mongo_backup_disk_keep_free	Percentage of disk that must be left free on the file system. The oldest backup files will be deleted when this limit is reached.	Yes	30
mongo_backup_start_time	Time of day when backup schedule starts in hh:mm+hh:mm or hh:mm-hh:mm format. First part of the format is the start time and second part is an offset (from UTC) for specifying the time zone. If the time zone is not specified, local time zone of the VM processing the request will be used as the default time zone.	Yes	02:00
mongo_backup_full_period	Interval at which the MongoDB full backups are performed. Expressed in weeks and/or days, or hours format, e.g. 1w2d or 4h. Hours cannot be provided with days or weeks. Maximum value for hour is 23h. 0 means that no backup is performed.	Yes	1d
mongo_backup_differential_period	Interval at which the MongoDB differential backups are performed. Expressed in weeks and/or days, or hours format, e.g. 1w2d or 4h. Hours cannot be provided with days or weeks. Maximum value for hour is 23h. 0 means that no backup is performed.	Yes	4h

Parameter	Description	Mandatory	Example
mongo_backup_retention	Time specifies how long to wait before deleting the file(s). Empty value means that we keep the files for 7 days. It is expressed in weeks, days and/or hours format, e.g. 1w24h or 2d. When retention is more than a day, the extra hours of a day would be trimmed and retention value would be rounded down to the closest day.	No	
etcd_existing_endpoints	Comma-separated list of existing etcd endpoint(s) <scheme>://<host address>:<client port>. For etcd clustering, this will take precedence over 'Existing VNF instances'	No	
etcd_data_volume_id	Identifier of the Cinder volume to use for etcd data.	No	
etcd_backup_volume_id	Identifier of the Cinder volume to use for etcd backup.	No	
etcd_root_password	Password for the etcd root user. This user has all access to etcd including creation of users, policies, removing kes store etc.	No	
etcd_user_name	Username for a etcd user. This user has read/write permission on path with same name.	No	
etcd_user_password	Password for the etcd user.	No	
etcd_client_cert	etcd GRPC client certificate. Used for init and etcdctl commands.	No	
etcd_client_key	etcd GRPC client private key. Used for init and etcdctl commands.	No	
etcd_client_ca_cert	etcd GRPC client CA certificate. Used for init and etcdctl commands.	No	

Parameter	Description	Mandatory	Example
etcd_server_cert	etcd GRPC server certificate. Used for grpc server.	No	
etcd_server_key	etcd GRPC server private key. Used for grpc server.	No	
etcd_server_ca_cert	etcd GRPC server CA certificate. Used for grpc server.	No	
etcd_peer_cert	etcd GRPC peer certificate. Used for clustering.	No	
etcd_peer_key	etcd GRPC peer private key. Used for clustering.	No	
etcd_peer_ca_cert	etcd GRPC peer CA certificate. Used for clustering.	No	
etcd_heartbeat_interval	Interval in ms at which the leader will notify followers that it is still the leader.	Yes	100
etcd_election_timeout	How long in ms a follower node will go for without hearing a heartbeat before attempting to become leader itself.	Yes	1000
etcd_backup_disk_max_use	Maximum percentage of the disk that may be occupied by etcd backup files.	Yes	15
etcd_backup_disk_keep_free	Percentage of disk that must be left free on the file system. The oldest backup files will be deleted when this limit is reached.	Yes	30
etcd_backup_start_time	Time of day when backup schedule starts in hh:mm+hh:mm or hh:mm-hh:mm format. First part of the format is the start time and second part is an offset (from UTC) for specifying the time zone. If the time zone is not specified, local time zone of the VM processing the request will be used as the default time zone.	Yes	02:00

Parameter	Description	Mandatory	Example
etcd_backup_full_period	Interval at which the etcd full backups are performed. Expressed in weeks and/or days, or hours format, e.g. 1w2d or 4h. Hours cannot be provided with days or weeks. Maximum value for hour is 23h. 0 means that no backup is performed.	Yes	0
etcd_backup_retention	Time specifies how long to wait before deleting the file(s). Empty value means that we keep the files for 7 days. It is expressed in weeks, days and/or hours format, e.g. 1w24h or 2d.	No	
prometheus_data_volume_id	Identifier of the Cinder volume to use for Prometheus and/or AlertManager data.	No	
prometheus_max_disk_usage_in_percent	Maximum disk usage allowed by Prometheus data in percent of the total disk size.	Yes	40
snmp_trap_target_ip	snmp trap target address.	Yes	10.34.146.134
snmp_trap_target_port	snmp trap target Port	Yes	162

To validate that services are running once the VM is ready, check the status of appservices using the following command as sysadm user.

```
$ vmccs-status
```

Example vmccs-status output:

```
$ vmccs-status
Validating backup-manager services status...
  backup-manager: active (running)
backup-manager is active

Validating Etcd services status...
  etcd: active (running)
Etcd is active
```

```

Validating Fluentbit services status...
  td-agent-bit: active (running)
  fluent-sd: active (running)
  fluent-sd-watch: active (running)
Fluentbit is active

Validating nginx services status...
  nginx: active (running)
  nginx-exporter: active (running)
nginx is active

Validating Node Exporter services status...
  node-exporter: active (running)
Node Exporter is active

Validating Prometheus services status...
  prometheus: active (running)
  prometheus-autoconfig: active (running)
  alertmanager: active (running)
  alertmanager-watch: active (running)
Prometheus is active

Validating SDR services status...
  sdr: active (running)
SDR is active

Validating VNF Operations services status...
  vnf-operations: active (running)
VNF Operations is active

All required vmCCS services are active.

```

Network **interface** roles

Default Gateway	Management	Internal	Signaling
eth0	eth0	eth0	eth0

Health Check etcd

You can check the status of cluster synchronization and health of any node.

Prerequisites

- The etcd is up and running.

Health check on etcd

- Log on as `root` user.
- Check the health of the cluster:

```
root@services3 ~]# etcdStatus.py
```

Name	ID	Endpoint	Leader	Healthy
services1	64386b664d63723b	http://172.29.86.21:2379	false	true
services2	81dcb39d0b4f7142	http://172.29.86.81:2379	true	true
services3	c88e907d0579400a	http://172.29.86.69:2379	false	true

etcd Alerts

In RAMP, to provide fault alerting, enable both the Prometheus and Alertmanager on the services VMs as part of a standard deployment. A Prometheus is a commonly used, open-source tool for retrieving real-time metrics. Alertmanager is a Prometheus component that manages notifications for alerts derived from Prometheus metrics. You can configure one or more SNMP destinations to receive traps derived from the Prometheus alerts. After you configure and enable an SNMP destination, use the management REST API to configure the SNMP destinations. For more information, refer [Updating the SNMP trapTarget](#).

The alerts generated by the Prometheus rules are expected to be sent to a *Prometheus AlertManager* instance. This AlertManager takes care of deduplicating, grouping, and routing the alerts to the correct destination. It is also possible to look at the currently active alerts using the AlertManager UI at <http://<alertmanager ip>:9093/>.

After deploying ETCD, login to any one of the ETCD and check the AlertManager and Prometheus details. The below command gives the AlertManager and Prometheus IP, username and password details. Use these details to log in to <https://<alertmanager IP>:9093/>.

Sample alertmanager configuration:

```
# curl -X GET http://127.0.0.1:8084/v1/config/nf/info 2>/dev/null | jq
{
  "alertmanager": {
    "password": "f1kLB,ov913i5wUv14bn20b=eo{}ZwWW",
    "url": [
      "https://172.19.52.129:9093",
      "https://172.19.52.139:9093",
      "https://172.19.52.209:9093"
    ],
    "username": "alertmanager"
  },
  "prometheus": {
    "password": "*8#aSIxLAKWRtdMr8H1{919,1UlwQ2Ch",
    "url": [
      "https://172.19.52.129:9090",
      "https://172.19.52.139:9090",

```

```

    "https://172.19.52.209:9090"
  ],
  "username": "prometheus"
}
}

```

List of Traps and Alerts

An overview of the various traps and alerts utilized within the RAMP are provided in this page, to monitor and manage application performance and security. Each entry includes a detailed description of the alert or trap, its purpose, and the necessary steps for resolution. All traps generated from the ETCD VM contain the following parameters:

- **trapUniqueId** – The OID of the trap.
- **trapSeverity** – The severity of the trap with one of the following values: critical, warning, or info. An info value is sent when an alert is cleared.
- **trapSummary** – A detailed description of the alert, including a list of all components impacted by the alert. If the list of impacted components changes, the system sends an updated alert. When the alert is cleared, the content is "Status: OK"

There are no explicit clear traps. To clear an alert, the system sends a trap with the same OID, but with a trapSeverity value of info. This section list the alerts that can be generated based on the metrics of AppServices VNF. All platform alerts can also be generated on this VNF.

Node Alerts

Name	Severity	Condition	SNMP OID
HostOutOfMemory	warning	< 10% free memory.	1.3.6.1.4.1.52694.1.1.1.1.0.1
HostMemoryUnderMemoryPressure	warning	> 1000 page faults per minute.	1.3.6.1.4.1.52694.1.1.1.1.0.2
HostUnusualNetworkThroughputIn	warning	Ingress traffic > 50 MB/s for over a minute.	1.3.6.1.4.1.52694.1.1.1.1.0.3
HostUnusualNetworkThroughputOut	warning	Egress traffic > 50 MB/s for over a minute.	1.3.6.1.4.1.52694.1.1.1.1.0.4
HostUnusualDiskReadRate	warning	Disk read > 50 MB/s for over a minute.	1.3.6.1.4.1.52694.1.1.1.1.0.5
HostUnusualDiskWriteRate	warning	Disk write > 50 MB/s for over a minute.	1.3.6.1.4.1.52694.1.1.1.1.0.6
HostOutOfDiskSpace	warning	< 10% free disk space for a partition.	1.3.6.1.4.1.52694.1.1.1.1.0.7

Name	Severity	Condition	SNMP OID
HostDiskWillFillIn4 Hours	critical	Linear prediction: expect disk partition to be full in the next 4 hours.	1.3.6.1.4.1.52694.1.1.1.1 .0.8
HostOutOfInodes	warning	< 10% free inodes.	1.3.6.1.4.1.52694.1.1.1.1 .0.9
HostUnusualDiskRead Latency	warning	Read latency > 100ms for over a minute.	1.3.6.1.4.1.52694.1.1.1.1 .0.10
HostUnusualDiskWrite Latency	warning	Write latency > 100ms for over a minute.	1.3.6.1.4.1.52694.1.1.1.1 .0.11
HostHighCpuLoad	warning	CPU usage over 80% for over 5 minutes.	1.3.6.1.4.1.52694.1.1.1.1 .0.12
HostSwapIsFillingUp	warning	> 80% swap memory used.	1.3.6.1.4.1.52694.1.1.1.1 .0.13
HostSystemdServiceCrashed	warning	The specified systemd service is in failed state.	1.3.6.1.4.1.52694.1.1.1.1 .0.14
HostKernelVersionDeviations	warning	Kernel version changed detected.	1.3.6.1.4.1.52694.1.1.1.1 .0.15
HostOomKillDetected	critical	Out-of-memory kill detected in the last 5 minutes.	1.3.6.1.4.1.52694.1.1.1.1 .0.16
HostNetworkReceiveErrors	warning	Ingress traffic error detected in the last 5 minutes.	1.3.6.1.4.1.52694.1.1.1.1 .0.17
HostNetworkTransmitErrors	warning	Egress traffic error detected in the last 5 minutes.	1.3.6.1.4.1.52694.1.1.1.1 .0.18
HostLowEntropy	warning	Entropy bits available is < 250.	1.3.6.1.4.1.52694.1.1.1.1 .0.19
PrometheusTargetMissing	critical	Exporter is not reporting metrics.	1.3.6.1.4.1.52694.1.1.1.1 .0.20

Name	Severity	Condition	SNMP OID
HostClockNotSynchronizing	warning	VM clock is not synchronized with NTP.	1.3.6.1.4.1.52694.1.1.1.1.0.21

SDR Alerts

Name	Severity	Condition	SNMP OID
SdrOutOfFileDescriptor	warning	> 90% available file descriptors used.	1.3.6.1.4.1.52694.1.1.1.3.0.2
SdrRegistryUnreachable	warning	SDR is unable to contact a service registry.	1.3.6.1.4.1.52694.1.1.1.3.0.3
SdrRegistryAllUnreachable	critical	SDR is unable to contact all service registries.	1.3.6.1.4.1.52694.1.1.1.3.0.4
PrometheusTargetMissing	critical	Exporter is not reporting metrics.	1.3.6.1.4.1.52694.1.1.1.3.0.1

Fluent Alerts

Name	Severity	Condition	SNMP OID
FluentOutputError	warning	Fluent is reporting output errors.	1.3.6.1.4.1.52694.1.1.1.2.0.2
PrometheusTargetMissing	critical	Exporter is not reporting metrics.	1.3.6.1.4.1.52694.1.1.1.2.0.1

Etcd Alerts

Name	Severity	Condition	SNMP OID
EtcdInsufficientMembers	critical	Etcd cluster should have an odd number of members.	1.3.6.1.4.1.52694.1.1.1.5.0.2

Name	Severity	Condition	SNMP OID
EtcdNoLeader	critical	Etcd cluster has no leader.	1.3.6.1.4.1.52694.1.1.1.5.0.3
EtcdHighNumberOfLeaderChanges	warning	Etcd leader changed more than 3 times during the last hour.	1.3.6.1.4.1.52694.1.1.1.5.0.4
EtcdHighNumberOfFailedGrpcRequests	warning	More than 1% GRPC request failures detected in Etcd for 5 minutes.	1.3.6.1.4.1.52694.1.1.1.5.0.5
	critical	More than 5% GRPC request failures detected in Etcd for 5 minutes.	1.3.6.1.4.1.52694.1.1.1.5.0.6
EtcdGrpcRequestsSlow	warning	GRPC requests slowing down, 99th percentile is over 0.15s for 5 minutes.	1.3.6.1.4.1.52694.1.1.1.5.0.7
EtcdHighNumberOfFailedHttpRequests	warning	More than 1% HTTP failures detected in Etcd for 5 minutes.	1.3.6.1.4.1.52694.1.1.1.5.0.8
	critical	More than 5% HTTP failures detected in Etcd for 5 minutes.	1.3.6.1.4.1.52694.1.1.1.5.0.9
EtcdHttpRequestsSlow	warning	HTTP requests slowing down, 99th percentile is over 0.15s for 5 minutes.	1.3.6.1.4.1.52694.1.1.1.5.0.10
EtcdMemberCommunicationSlow	warning	Etcd member communication slowing down, 99th percentile is over 0.15s for 5 minutes.	1.3.6.1.4.1.52694.1.1.1.5.0.11
EtcdHighNumberOfFailedProposals	warning	Etcd server got more than 5 failed proposals in the past hour.	1.3.6.1.4.1.52694.1.1.1.5.0.12
EtcdHighFsyncDurations	warning	Etcd WAL fsync duration increasing, 99th percentile is over 0.5s for 5 minutes.	1.3.6.1.4.1.52694.1.1.1.5.0.13
EtcdHighCommitDurations	warning	Etcd commit duration increasing, 99th percentile is over 0.25s for 5 minutes.	1.3.6.1.4.1.52694.1.1.1.5.0.14
PrometheusTargetMissing	critical	Exporter not reporting metrics / Etcd instance unreachable.	1.3.6.1.4.1.52694.1.1.1.5.0.1

Prometheus Alerts

Name	Severity	Condition	SNMP OID
PrometheusTargetMissing	critical	Exporter not reporting metrics.	1.3.6.1.4.1.52694.1.1.1.7.0.1
PrometheusAllTargetsMissing	critical	Prometheus does not have a reachable target.	1.3.6.1.4.1.52694.1.1.1.7.0.2
PrometheusConfigurationReloadFailure	warning	Prometheus configuration reload failure.	1.3.6.1.4.1.52694.1.1.1.7.0.3
PrometheusTooManyRestarts	warning	Prometheus has restarted more than twice in the last 15 minutes and might be crashlooping.	1.3.6.1.4.1.52694.1.1.1.7.0.4
PrometheusNotConnectedToAlertmanager	critical	Prometheus cannot connect the Alertmanager.	1.3.6.1.4.1.52694.1.1.1.7.0.5
PrometheusRuleEvaluationFailures	critical	Prometheus encountered rule evaluation failures, potentially leading to ignored alerts.	1.3.6.1.4.1.52694.1.1.1.7.0.6
PrometheusTemplateTextExpansionFailures	critical	Prometheus template text expansion failures.	1.3.6.1.4.1.52694.1.1.1.7.0.7
PrometheusRuleEvaluationSlow	warning	Prometheus rule evaluation took more time than the scheduled interval.	1.3.6.1.4.1.52694.1.1.1.7.0.8
PrometheusNotificationsBacklog	warning	The Prometheus notification queue has not been empty for 10 minutes.	1.3.6.1.4.1.52694.1.1.1.7.0.9
PrometheusTargetScrapingSlow	warning	Prometheus is scraping exporters slowly.	1.3.6.1.4.1.52694.1.1.1.7.0.10
PrometheusLargeScrape	warning	Prometheus has many scrapes that exceed the sample limit.	1.3.6.1.4.1.52694.1.1.1.7.0.11

Name	Severity	Condition	SNMP OID
PrometheusTargetScrapeDuplicate	warning	Prometheus rejected many samples due to duplicate timestamps, but different values.	1.3.6.1.4.1.52694.1.1.1.7.0.12
PrometheusTsdbCheckpointCreationFailures	critical	Prometheus encountered time-series database (TSDB) checkpoint creation failures.	1.3.6.1.4.1.52694.1.1.1.7.0.13
PrometheusTsdbCheckpointDeletionFailures	critical	Prometheus encountered TSDB checkpoint deletion failures.	1.3.6.1.4.1.52694.1.1.1.7.0.14
PrometheusTsdbCompactionsFailed	critical	Prometheus encountered TSDB compaction failures.	1.3.6.1.4.1.52694.1.1.1.7.0.15
PrometheusTsdbHeadTruncationsFailed	critical	Prometheus encountered TSDB head truncation failures.	1.3.6.1.4.1.52694.1.1.1.7.0.16
PrometheusTsdbReloadFailures	critical	Prometheus encountered TSDB reload failures.	1.3.6.1.4.1.52694.1.1.1.7.0.17
PrometheusTsdbWALCorruptions	critical	Prometheus encountered TSDB write-ahead log (WAL) failures.	1.3.6.1.4.1.52694.1.1.1.7.0.18
PrometheusTsdbWALTruncationsFailed	critical	Prometheus encountered TSDB WAL truncation failures.	1.3.6.1.4.1.52694.1.1.1.7.0.19

Alertmanager Alerts

Name	Severity	Condition	SNMP OID
PrometheusTargetMissing	critical	Exporter not reporting metrics.	1.3.6.1.4.1.52694.1.1.1.8.0.1
AlertmanagerConfigurationReloadFailure	warning	Alertmanager configuration reload error.	1.3.6.1.4.1.52694.1.1.1.8.0.2

Name	Severity	Condition	SNMP OID
AlertmanagerConfigNotSynced	warning	The configurations of Alertmanager cluster instances are out of sync.	1.3.6.1.4.1.52694.1.1.1.8.0.3
AlertmanagerNotificationFailing	critical	Alertmanager is failing to send notifications.	1.3.6.1.4.1.52694.1.1.1.8.0.4
AlertmanagerTooManyRestarts	warning	Alertmanager has restarted more than twice in the last 15 minutes and might be crashlooping.	1.3.6.1.4.1.52694.1.1.1.8.0.5

Nf-Operations Alerts

Name	Severity	Condition	SNMP OID
PrometheusTargetMissing	critical	Exporter not reporting metrics.	1.3.6.1.4.1.52694.1.1.1.9.0.1
nfUsageReportUploadedQueued	warning	Usage reports are not uploading.	1.3.6.1.4.1.52694.1.1.1.9.0.2
nfPrometheusConnectionFailing	critical	Connection to all Prometheus instances is failing, cannot fetch data.	1.3.6.1.4.1.52694.1.1.1.9.0.3

Nginx Alerts

Name	Severity	Condition	SNMP OID
PrometheusTargetMissing	critical	Exporter not reporting metrics / Nginx target is missing.	1.3.6.1.4.1.52694.1.1.1.10.0.1

Backup-Manager exporter alerts

Name	Severity	Condition	SNMP OID
PrometheusTargetMissing	critical	Exporter not reporting metrics.	1.3.6.1.4.1.52694.1.1.1.11.0.1

Name	Severity	Condition	SNMP OID
BackupmanagerScheduleFailed	critical	Backup-manager has failed to run a schedule in the last four hours	1.3.6.1.4.1.52694.1.1.1.1.0.2
SendBackupToSftpFailure	critical	Backup-manager has failed to send the backup file to SFTP location in the last hour	1.3.6.1.4.1.52694.1.1.1.1.0.3

SNMP Heartbeat Trap

If configured, the SNMP agent sends a heartbeat trap at a specified interval to your SNMP destination to verify the connection remains active. The following table provides details on the heartbeat trap. Refer to [Updating the SNMP trapTarget](#) for information on configuring the heartbeat trap interval.

SNMP Heartbeat Trap

Trap	Severity	Triggering Event	SNMP OID
clusterHeartbeat	info	Trap sent at a regular interval to allow the destination to monitor that this network function remains present and accessible.	1.3.6.1.4.1.52694.1.1.1.6.0.1

Updating the SNMP trapTarget

In this section:

- [SNMP Authentication and Encryption Parameters](#)
- [SNMP Destination Parameters](#)
- [Heartbeat Parameter](#)
- [Create a New SNMPv3 Destination](#)
- [Create a New SNMPv2c Destination](#)
- [Work with Existing SNMP Destination Configuration](#)
 - [Retrieve Existing SNMP Destinations](#)
 - [Edit an Existing SNMP Destination](#)
 - [Delete an Existing SNMP Destination](#)
- [Work with Existing SNMP User Configuration](#)
 - [Retrieve Existing SNMP Users](#)
 - [Edit an Existing SNMP User](#)
 - [Delete an Existing SNMP User](#)
- [Configure an SNMP Heartbeat Interval](#)

- [Retrieve the Current Heartbeat Configuration](#)

Ribbon Service app supports specifying one or more external SNMP destinations to which you want to send traps derived from Prometheus alerts. If you are using SNMP in your network, Service app also provides an option to configure an SNMP "heartbeat" to monitor the connection between the Service app deployment and your SNMP destination. When configured, the heartbeat mechanism triggers a heartbeat alert at an interval you specify so that the SNMP destination regularly receives traps that confirm the connection is active.

Service app supports sending traps in both SNMPv2c and SNMPv3 formats. The version type of the destination determines which parameters you must configure for the destination. An SNMPv3 destination requires both authentication and encryption parameters and general SNMP destination parameters. An SNMPv2c destination requires only general SNMP destination parameters. The following tables describe these parameters.

SNMP Authentication and Encryption Parameters

The following table describes the authentication and encryption parameters required by SNMPv3 and defined within the `snmpUser` object in the API.

SNMP Authentication and Encryption Parameters

Parameter	Description
<code>authPassphrase</code>	This parameter specifies an SNMP authentication passphrase. Include this parameter if you are enabling authentication.
<code>authProtocol</code>	This parameter specifies the SNMP authentication protocol. Specify either <code>MD5</code> or <code>SHA</code> , or use an empty string to disable authentication.
<code>name</code>	This parameter specifies the name of this SNMP security user definition. Specify this name as the <code>securityName</code> in the general SNMP destination parameters to associate this set of authentication and encryption settings with the destination. This parameter is required within the body of a POST (add) request and is included in the path of a PUT (update) request.
<code>privPassphrase</code>	This parameter specifies an SNMP privacy passphrase. Include this parameter if you are enabling encryption.
<code>privProtocol</code>	This parameter specifies the SNMP privacy protocol. Specify either <code>DES</code> or <code>AES-128</code> , or use an empty string to disable encryption.

SNMP Destination Parameters

The following table describes the SNMP destination parameters defined within the `snmpDestination` object in the API. The final two columns (X=supported) indicate whether a parameter applies to SNMPv2c, SNMPv3, or both SNMP versions.

SNMP Destination Parameters

Parameter	Description	v2c	v3
community	This parameter specifies the SNMP community string. The default value is <code>public</code> .	X	
contextEngineId	This parameter specifies the SNMP context engine ID. If not specified, this defaults to the security engine ID.		X
contextName	This parameter specifies the SNMP context name used to address a specific instance of a managed object.		X
host	This parameter identifies the host of the SNMP destination. The value can be either an IP address or an FQDN. An FQDN will be resolved using service discovery.	X	X
name	This parameter assigns a name to this SNMP destination definition and is used by the API. This parameter is required within the body of a POST (add) request and is included in the path of a PUT (update) request.	X	X
port	This parameter specifies the target port on the SNMP destination. The range allowed is 1 to 65535 and the default value is <code>162</code> .	X	X
securityEngineId	This parameter specifies the SNMP security engine ID.		X
securityName	This parameter specifies the SNMP security username and must match a name assigned to an <code>snmpUser</code> object. This associates the authentication and encryption settings for the specified <code>snmpUser</code> with this destination.		X
state	This parameter specifies the state of the SNMP destination. The values allowed are <code>enabled</code> or <code>disabled</code> . The Service app SNMP agent does not send traps to a disabled destination. The default value is <code>enabled</code> .	X	X
version	This parameter specifies the version of the SNMP protocol to use for this destination. The values allowed are <code>v3</code> and <code>v2c</code> . The default value is <code>v2c</code> .	X	X

Heartbeat Parameter

The following table describes the heartbeat interval parameter defined with the `heartbeat` object in the API.

Heartbeat Parameter

Parameter	Description
<code>interval</code>	This parameter specifies the interval, in seconds, at which Service app SNMP agent triggers a heartbeat alert as a mechanism for monitoring the connection between the Service app deployment and SNMP destinations. 0 means the alert is disabled and is the default value.

Create a New SNMPv3 Destination

To create a new SNMPv3 destination, you must first define an SNMP security user (`snmpUser`) to specify authentication and encryption settings. Then, include the name you assigned to the SNMP security user within the general SNMP destination configuration (`snmpDestination`) to associate the authentication and encryption settings with the destination.

1. Use curl to submit the following request to create an SNMP security user. Use the descriptions in the first table above to define the SNMP security user settings to include in your request.

```
POST <127.0.0.1>:8084/v1/config/nf/snmp/users
```

2. Use curl to submit the following request to create an SNMP destination. Use the descriptions in the second table above to define the settings for the destination. Be sure to include the name of the appropriate SNMP security user as the `securityName` in your request, as well as the other parameters applicable to SNMPv3, as appropriate.

```
POST <127.0.0.1>:8084/v1/config/nf/snmp/destinations
```

Create a New SNMPv2c Destination

To create an SNMPv2c destination, you must define appropriate general SNMP destination settings (`snmpDestination`).

Use curl to submit the following request to create an SNMP destination. Use the descriptions in the second table above to define the settings for the destination. Be sure to include the parameters applicable to SNMPv2c, as appropriate.

```
POST <127.0.0.1>:8084/v1/config/nf/snmp/destinations
```

Example to add snmp traptarget

Sample output to add snmp traptarget:

```
$ curl -H 'Content-Type: application/json' \
  -d '{ "name": "snmptarget-1", "host": "10.34.146.134", "port": 162, "version": "v2c",
    "community": "public" }' \
```

```
-X POST \  
http://127.0.0.1:8084/v1/config/nf/snmp/destinations
```

To check the SNMP trapTargets, use the below command:

```
$ curl -X GET http://127.0.0.1:8084/v1/config/nf/snmp/destinations  
[{"community":"public","host":"10.34.146.134","name":"snmptarget-1","port":162,"state":"  
enabled","version":"v2c"}]
```

Work with Existing SNMP Destination Configuration

You can use the API to return the settings for currently configured SNMP destinations, make updates to the configurations, or to delete a destination.

Retrieve Existing SNMP Destinations

Use curl to submit the following request to return the list of currently configured SNMP destinations.

```
GET <127.0.0.1>:8084/v1/config/nf/snmp/destinations
```

The command returns the set of SNMP destinations currently stored in the ETCD.

Use curl to submit the following request to return the configuration for the SNMP destination matching the `name` you specify.

```
GET <127.0.0.1>:8084/v1/config/nf/snmp/destinations/{name}
```

The command returns the configuration for the specific SNMP destination you specified.

Edit an Existing SNMP Destination

Use curl to submit the following request to update the configuration of the SNMP destination matching the `name` you specify.

```
PUT <127.0.0.1>:8084/v1/config/nf/snmp/destinations/{name}
```

The command updates the values for the parameters you include in your request in the configuration of the SNMP destination you specified.

Delete an Existing SNMP Destination

Use curl to submit the following request to delete the SNMP destination matching the `name` you specify.

```
DELETE <127.0.0.1>:8084/v1/config/nf/snmp/destinations/{name}
```

The command deletes the SNMP destination you specified.

Work with Existing SNMP User Configuration

You can use the API to return the settings for currently configured SNMP users, make updates to the configurations, or to delete an SNMP user.

Retrieve Existing SNMP Users

Use curl to submit the following request to return the list of currently configured SNMP users.

```
GET <127.0.0.1>:8084/v1/config/nf/snmp/users
```

The command returns the set of SNMP users currently stored in the ETCD.

Use curl to submit the following request to return the configuration for the SNMP users matching the `name` you specify.

```
GET <127.0.0.1>:8084/v1/config/nf/snmp/users/{name}
```

The command returns the configuration for the specific SNMP user you specified.

Edit an Existing SNMP User

Use curl to submit the following request to update the configuration of the SNMP user matching the `name` you specify.

```
PUT <127.0.0.1>:8084/v1/config/nf/snmp/users/{name}
```

The command updates the values for the parameters you include in your request in the configuration of the SNMP user you specified.

Delete an Existing SNMP User

Use curl to submit the following request to delete the SNMP user matching the `name` you specify.

```
DELETE <127.0.0.1>:8084/v1/config/nf/snmp/users/{name}
```

The command deletes the SNMP user you specified.

Configure an SNMP Heartbeat Interval

Use curl to submit the following request to specify an interval, in seconds, at which ETCD sends a heartbeat alert. When set to 0 (default) the heartbeat alert is disabled.

```
POST <127.0.0.1>:8084/v1/config/nf/heartbeat
```

Retrieve the Current Heartbeat Configuration

Use curl to submit the following request to return the current heartbeat configuration.

```
GET <127.0.0.1>:8084/v1/config/nf/heartbeat
```

RAMP etcd System Requirements

In this section:

- [Resource Requirements](#)
- [Environment-Specific Minimum Resource Requirements](#)

The system requirements for deploying `etcd` on the Ribbon Application Management Platform (RAMP) are described below.

Resource Requirements

This table covers the minimum resource requirements for a single `etcd` instance. Use three instances with this configuration for a three-node `etcd`.

Resource	Environment			
	KVM	VMware ESXi	OpenStack	CNF
Disk (GB)	50		50 (HDD)	21 (external volume)
RAM (GB)	2			3
vCPU	1			2
vNIC	1			
Network attributes				
Max round-trip-time	100 ms			

Environment-Specific Minimum Resource Requirements

Environment-specific minimum resource requirements for `etcd` are covered in this table.

Environment	Resource	Version		
KVM	KVM (Kernel Virtual Machine)	3.10.0		
	Compilation library	libvirt 4.5.0		
	Library	libvirt 4.5.0		
	API	QEMU 4.5.0		
	Hypervisor	QEMU 1.5.3		
VMware	VMware ESXi	6.5	6.7	7.0
	Virtual Machine	13	14	14
	Hard Disk Type	Thick provisioned, lazily zeroed.		

Environment	Resource	Version
OpenStack	Red Hat OpenStack Platform (RHOSP)/ Host operating system	• 10 / RHEL 7.3 • 13 / RHEL 7.5 • 16 & 16.1/ RHEL 8.1

Lawful Intercept Guide

Contents

- [Ribbon Lawful Intercept Overview](#)
- [Lawful Intercept for RAMP](#)
- [Enabling Lawful Intercept on RAMP](#)
- [Configuring Call Data Channel](#)
 - [Configure CDC for All Nodes](#)
 - [Configure CDC for GSX Nodes](#)
 - [Configure CDC for SBC Core Nodes](#)
- [Managing Mediation Servers](#)
 - [Create a Mediation Server](#)
 - [Importing TLS Security Certificate to RAMP](#)
- [Provisioning LI Targets](#)
 - [Target Provisioning Sequence](#)
 - [Apply Restrictions on Lawful Intercept Targets](#)
- [Call Processing](#)
 - [Call Data Interface](#)
 - [Call Content Interface](#)
 - [GSX Lawful Intercept Basic Call Processing](#)
 - [SBC Lawful Intercept Basic Call Processing](#)
- [Viewing CDC Status Report](#)
 - [View GSX CDC Report Using CLI](#)
- [LI Performance Management](#)
 - [GSX LI Performance Reports](#)
 - [SBC LI Performance Reports](#)
- [LI Fault Management](#)
 - [GSX Lawful Intercept Alarms](#)
 - [SBC Lawful Intercept Alarms](#)
 - [RAMP Lawful Intercept Alarms](#)
- [LI Security](#)
- [Deploying liTestWebApp in RAMP](#)
- [Related Documentation](#)

This guide provides information on using Ribbon Application Management Platform (RAMP) as part of the Ribbon Lawful Intercept solution.

Ribbon Lawful Intercept Overview

In this section:

- [Ribbon Lawful Intercept Topology](#)
 - [Intercept Server](#)
 - [SBC Network Border Switch](#)

- [PSX Policy Server](#)

Statutes such as the Communication Assistance for Law Enforcement Act (CALEA, 1994, United States) define the ability of law enforcement to intercept wire and electronic communications and obtain call data and call content for calls under surveillance.

Telecom carriers may have to provide the means to collect call data and call content (voice streams) from their customers in response to lawful authorization. The core of this ability is provided by an Intercept Server (IS) at the carrier's premises that formats call content and data according to various national standards.

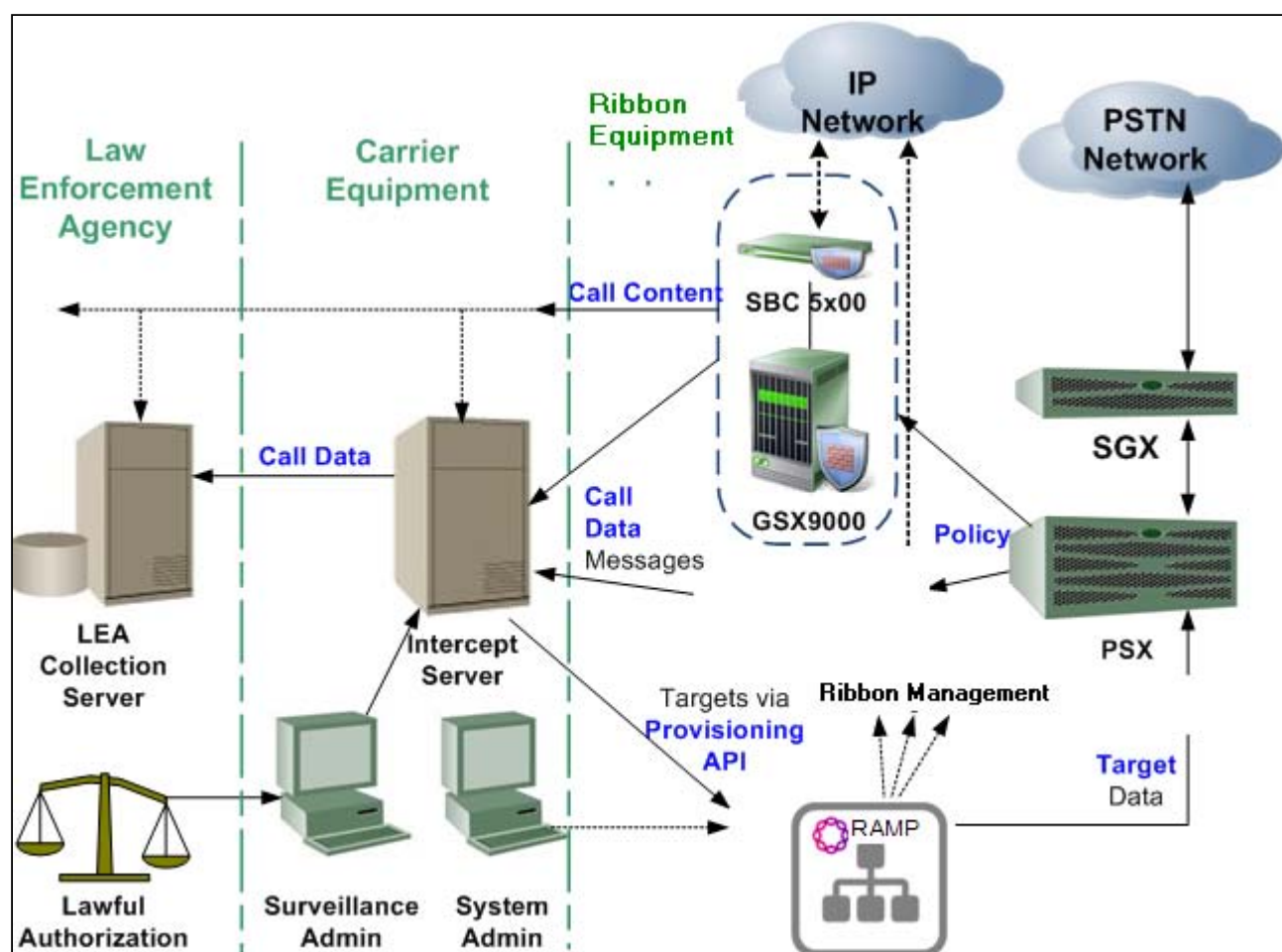
The IS is provisioned with specific targets, typically subscriber phone numbers. When the carrier's equipment detects the start of a call involving a target, it sends messages to the IS at various stages of the call. It also taps into the voice streams and sends copies of them to an IP address designated by the IS, if so configured. The IS then forwards call data and call content on to law enforcement Delivery Function (DF) devices at the LEA premises, which will filter as appropriate per outstanding warrants.

The carrier's equipment, such as that supplied by Ribbon Communications, is capable of identifying calls involving the provisioned targets and collect call data and content, without the callers being aware.

The Ribbon Lawful Intercept solution is an integrated system for identifying LI targets, collecting call data and content, and forwarding it to Law Enforcement Agency. It includes an Intercept Server from partners. The Intercept Server provides the human interface for provisioning. It provides a fan out capability so that multiple Law Enforcement Agencies (LEAs) can intercept each target. It also communicates with network provider intercept equipment.

Ribbon Lawful Intercept Topology

This section describes the network topology of the Ribbon Lawful Intercept (LI) solution.



In a Ribbon deployment, calls may arrive at the SBC Core for VoIP calls.

The following call information can be collected:

- **Call content**
The real-time audio streams of a call under surveillance, forwarded from the SBC Core to the address provided by the IS.

The call under surveillance is unaware of this wiretap.

- **Call data**
A series of real-time call-identifying information messages sent from an SBC Core device to the IS.

Intercept Server

Intercept server (IS) or Mediation Device is supplied by a Ribbon partner or the carrier. The IS interfaces to one or more law enforcement agencies, and to other network provider intercept equipment.

IS has interfaces to Ribbon equipment for provisioning, call data, and call content. IS serves as the carrier's interface for provisioning intercept targets in response to lawful target authorization requests. It formats this data as necessary and communicates it via the Lawful Intercept API to Ribbon Application Management Platform (RAMP).

Intercept server interacts with RAMP for all provisioning. RAMP distributes this provisioning to all other Ribbon devices as needed. IS interacts with the Ribbon network element for call data and call content.

When the SBC Core identifies a call to be trapped, the devices send Call Data messages to the IS at various stages of the call. In response, the IS tells the SBC the IP address and port number(s) to send the collected call content RTP streams.

When the SBC Core devices identify a call to be trapped, the devices send Call Data messages to the IS at various stages of the call. In response, the IS triggers the SBC devices to send the collected call content RTP streams using the IP address and ports.

RAMP

RAMP receives and processes Lawful Intercept target provisioning data from the IS via SOAP-based API.

RAMP then distributes this data to all primary PSX devices, and generates success or failure responses to IS. Ribbon Lawful Intercept solution allows you to manage the lawful intercept capabilities of the Intercept Server/Mediation device.

RAMP, PSX, and SBC Core

You can access the following through Lawful Intercept shortcut in RAMP:

Note

Lawful Intercept shortcut is visible only if the Lawful Intercept license has been applied to RAMP and you have Lawful Intercept privileges.

- CDC Provisioning interface:
It allows you to configure the IP address, UDP port, and other parameters used for communication between the Ribbon devices and the intercept server.
- Report interface:
It retrieves and displays CDC information for all the nodes.

SBC Network Border Switch

After call information arrives, SBC sends a policy request to PSX. When directed by the policy response from the PSX, the SBC acts as an intercept access point (IAP) and establishes a Call Data channel for messages and status over UDP/IP to the Intercept Server. SBC also sends the call voice streams (call content) RTP copy to an IP address provided by the IS.

PSX Policy Server

PSX maintains the database of all subscribers, including the provisioning information from the IS as relayed by RAMP. When the call parameters in a policy request (for example, Called or Calling Number) from the SBC Core devices matches any provisioned Lawful Intercept criteria, the PSX adds information about the matching LI criteria to its policy response to the SBC Core.

Lawful Intercept for RAMP

The Lawful Interception solution has three discrete interfaces between the network element and mediation server to provide provisioning, call data (signaling) and call content (media) information. These interfaces are created after the connection is established between the mediation server Delivery Function (DF) and the network

element Access Function (AF). The Mediation Function (MF) provides the required interworking by interfacing to the Law Enforcement Agency (LEA) through Handover Interfaces (HI1, HI2, HI3) on one side and to the VoIP packet network element(s) through X3 (for collection of media). The interface from the mediation server to the lawful interception agency is standardized. The interfaces between AF and DF are defined as:

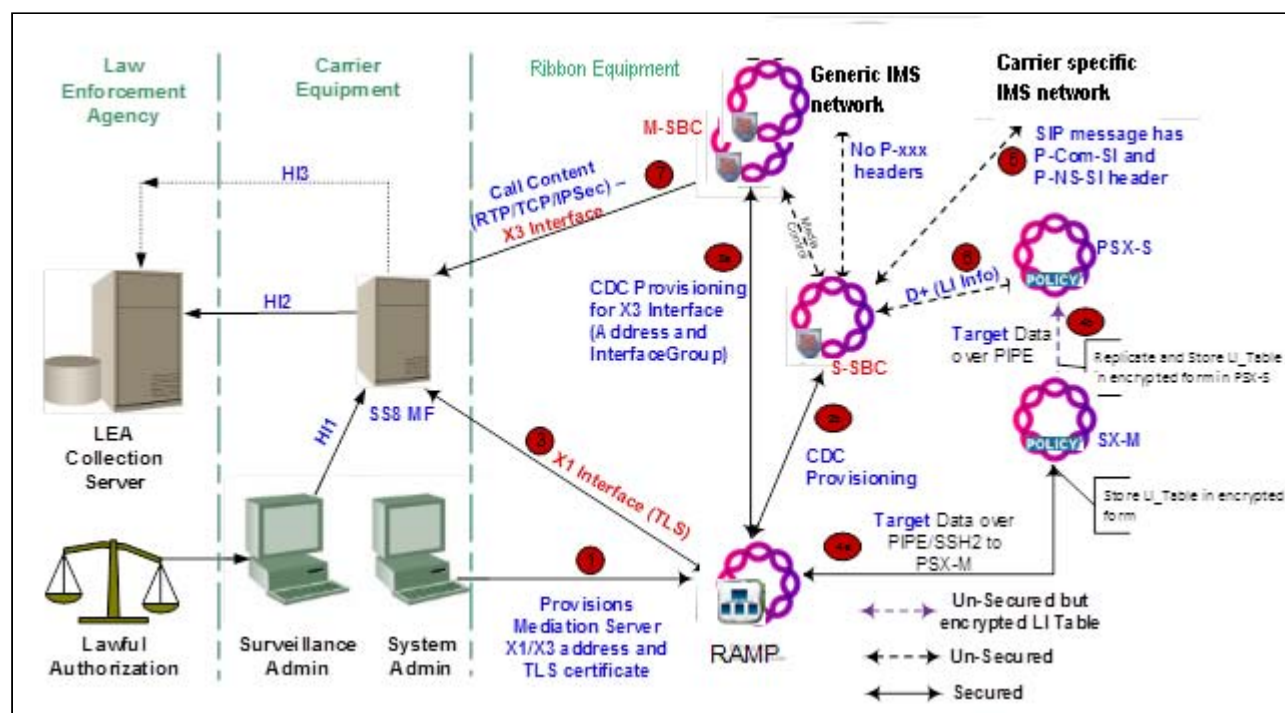
- X1 or INI-1 interface is supported by Ribbon Application Management Platform (RAMP) for provisioning targets and the targets data is stored in PSX database. This is based on SS8 provisioning interface.

Where, X interface is specified by 3GPP standard while INI is specified by ETSi standard.

Lawful Interface Architecture

Following is the P-Com.Session-Info LI architecture which consists of Ribbon network elements (RAMP, PSX, S-SBC, and M-SBC) with SS8 as the mediation server. The Ribbon LI solution supports only X1 and X3 interfaces.

Lawful Intercept Topology



The Intercept server has interfaces to Ribbon equipment for provisioning and call content. The Intercept Server interacts with RAMP for provisioning and with network element for call content. RAMP acts as a AF (Administrative Function) from an SS8 mediation function perspective to terminate provisioning of the targets. The SBC acts as CC IAPs (call content IAPs) for bearer interception. SS8 is only applicable for a customer-specific deployment.

For SBC Core LI flavors, refer to [Lawful Intercept](#).

Enabling Lawful Intercept on RAMP

To intercept media packets, Ribbon Application Management Platform (RAMP) must be either the same version or a higher version as that of the SBC and PSX devices.

Start

1. Access RAMP as the insight user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the insight user.

2. Stop RAMP:

```
/opt/sonus/ems/emsMgmt stop
```

3. Edit the `/opt/sonus/ems/weblogic/sonusEms/data/sys/SystemConfig.txt` file and add `defaultCaleaUser=true`.

This creates a default "calea" user in RAMP with LI privileges and a default password "calea".

4. Start RAMP:

```
/opt/sonus/ems/emsMgmt start
```

5. Log on to RAMP GUI as "calea" user with the default password.
6. Change the default "calea" password.
7. You can create additional user account(s) with CALEA privileges.

The username and password of an account with CALEA privileges will be configured in the IS and sent in the header of each LI API provisioning message.

8. Install RAMP-LI license on RAMP. For more information on the license, refer to [Node Locked Licenses on RAMP](#).
9. Create one or more users with LI privileges on RAMP.
10. Configure Call Data Channel (CDC) information on the SBC devices.
11. Configure the Intercept Server, per its manufacturer's instructions, to enable sending LI target information through the LI API.

Lawful Intercept under **OBSERVABILITY** in RAMP GUI is visible only if a PSX or SBC device is registered.

When you log on to RAMP GUI with CALEA privileges, **Lawful Intercept** will appear in the **OBSERVABILITY** tab.

After LI is established on the Ribbon equipment, you can use the existing RAMP Performance Manager and Fault Manager interfaces to monitor the system.

Configuring Call Data Channel

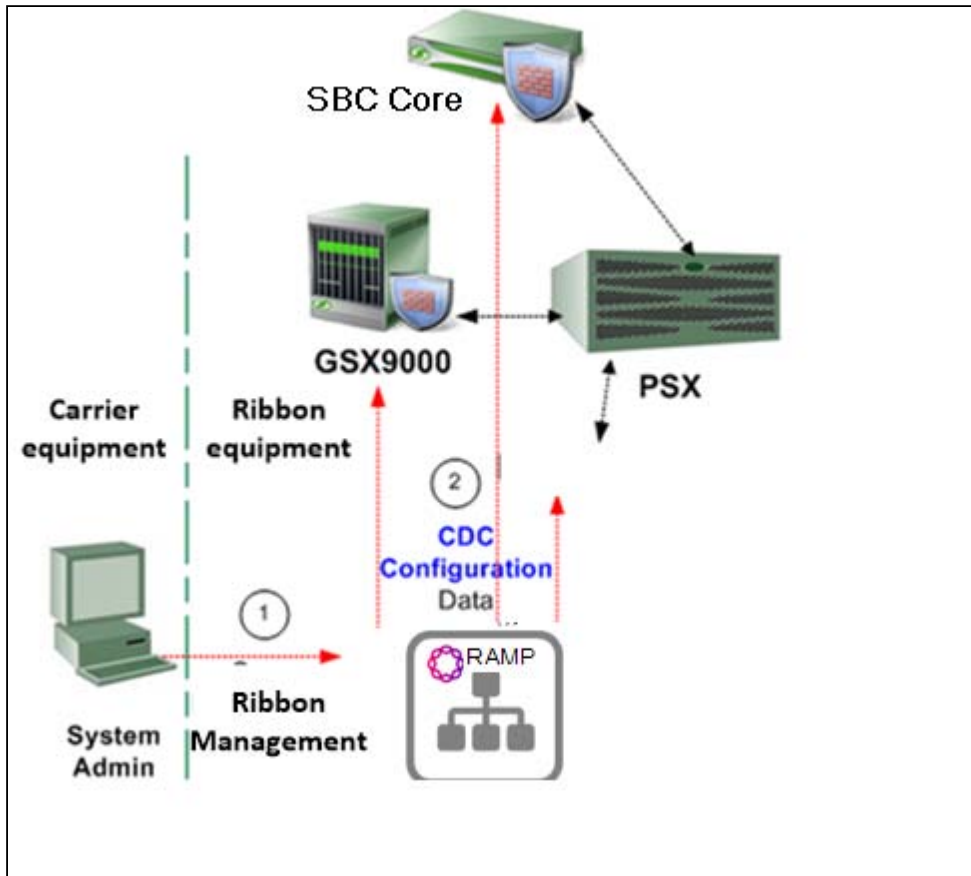
In this section:

- [Configure CDC for All Nodes](#)
- [Configure CDC for GSX Nodes](#)
- [Configure CDC for SBC Core Nodes](#)
 - [Configure CDC for an SBC Core Node](#)
 - [Configuring CDC for SBC SWe on Cloud](#)
 - [Configuring Mediation Server for SBCs](#)

- [Delete a Mediation Server Created for SBC Core](#)

Use Ribbon Application Management Platform (RAMP) to configure the Ribbon network elements and point them at the appropriate mediation devices for call data and call content delivery.

CDC Configuration



The Network Element ID generated and assigned by RAMP identifies every Ribbon network element. If necessary, configure assigned NE IDs in the partner's mediation device.

Note

Configure IS/MD with the assigned Network Element IDs.

Note

Configure CDC information for the SBC Core devices to perform Call Data and Call Content delivery for intercepted calls.

Every Ribbon SBC Core device is statically associated with a specific intercept server/mediation device (IS/MD) as a Call Data Channel entity. You must configure the SBC Core device with Call Data Channel (CDC) information to perform their LI function.

An authorized LI provisioner can select a SBC Core device and enter the relevant CDC information and configure the SBC Core device.

The Ribbon network element sends one message at a time to the intercept server. The Ribbon network element ensures reliable and ordered delivery of messages to the intercept server by retransmitting unacknowledged messages, based upon configuration.

Multiple network element may send call data messages to the intercept server for a single intercepted call. Since these call data messages use the same intercept criteria, the intercept server can correlate these messages. If more than one party in a call is an intercept target, the Ribbon network element delivers the call data for each target separately using different intercept criteria.

Every Ribbon network element sends a Media Report message to the intercept server with the following channel states:

- Open – Start call content delivery
- Close – End call content delivery

Note

RAMP supports adding up to 16 mediation servers in the Call Data Channel (CDC) for IMS LI.

Configure CDC for All Nodes

Use the following procedure to configure Call Data Channel (CDC) for all the SBC Core\GSX nodes in Ribbon Application Management Platform (RAMP). If any nodes are already configured, the new configuration replaces the existing one.

Prerequisites

Nodes are registered with RAMP.

Start

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC**.
3. Select or enter the values. Refer to [Configure CDC Device parameters](#).
4. Click **Configure All Devices**.

Configure CDC Device Parameters

Attribute	Description	Value range
Primary IP	The IP address of the mediation device. The Ribbon network element sends the call data to this IP Address. The IP address of the port being used is included in every call data message. The intercept server responds to these messages using the IP address received from the network element. The network element sends one message at a time to the intercept server.	A valid IPv4 address.
UDP Port	UDP port on the mediation device. The network element sends the call data to this UDP Port.	1 to 65535
Secondary IP (optional)	The secondary IP address of the mediation device.	A valid IPv4 address.
Keep Alive Timer	Interval for CDC keep-alive messages from the network element to the mediation device.	0 to 65535
Keep Alive Retries	Number of retries for keep-alive messages.	1 to 10
NIF/ IP Interface Group Name (Applicable for GSX and SBC only)	Specifies the name of the Network Interface group on the GSX or SBC.	Up to 23 alphanumeric characters
Send Noa Param (Version >= 8.3.0)	Specifies whether to send Nature of Address (NoA) information for E.164 numbers. Note The parameter applies only to the GSX.	- ENABLED - DISABLED (Default)
Server Type (Applicable for GSX only)	Specifies the name of the mediation device server type.	Default: Used for the default VERINT functionality. Zeel: Use this parameter when ZEEL mediation device is used for LI.

Configure CDC for GSX Nodes

To configure CDC for GSX nodes:

1. Log on to the Ribbon Application Management Platform (RAMP) as CALEA user.
2. Click **Monitoring > Lawful Intercept**. The **Lawful Intercept CDC Provisioning** window appears.
3. Click **Configure CDC** on the left navigation pane. The **Lawful Intercept/Configure CDC** window appears.
4. Perform the following steps to configure a GSX node or all the GSX nodes, as applicable:
 - To configure CDC for a specific GSX node:
 - i. Expand **GSXs** in the navigation pane and click **Configured** or **Non Configured**.
 - ii. Click on a node. The **Configure CDC Device** window appears.
 - iii. Select or enter the values. Refer to the table below for additional information.
 - iv. Click **Configure GSX**.
 - To configure CDC for all the GSX nodes:
 - i. Click **GSXs** in the navigation pane. The following window appears.
 - ii. Select or enter the values. Refer to the table below for additional information.
 - iii. Click **Configure All GSXs**.

Attribute	Description	Value range
Gateway Name	Gateway name for the node.	
Network Element ID	The Network Element ID uniquely identifies each Ribbon network element. Network Element ID is generated and assigned by the RAMP during the node registration process. The Network Element ID is included in the Call Data sent to the IS/MD. The IS/MD determines the origination point for the intercept (the SBC or GSX). You need to configure the partner's mediation device separately to identify the assigned NE IDs, if necessary. The system includes the node number in every CDC message as per the PacketCable PKT-SP-EM-I08-040113 specification.	0 to 99999
Node Number	The global unique node number for the SBC used by the LI Server for ID.	
Send Noa Param (Version >= 8.3.0)	Specifies whether to send Nature of Address (NoA) information for E.164 numbers. This field is used to enable or disable the Nature of Address (NoA) support.	• ENABLED • DISABLED (Default)
Server Type (Version >= 9.0)	Specifies the name of the mediation device server type. The attribute is available from Release 9.0 and later.	• Default: Used for the default VERINT functionality. • Zeel: Use this parameter when ZEEL mediation device is used for LI.

Attribute	Description	Value range
Primary IP	The IP address of the Lawful Intercept device.	A valid IPv4 address
UDP Port	UDP port on the mediation device. The Ribbon network element sends the call data to this UDP Port.	1 to 65535
Secondary IP	(optional) Secondary IP address of the mediation device.	
Keep Alive Timer	Interval for CDC keep alive messages from the Ribbon network element to the mediation device.	0 to 65535
Keep Alive Retries	Number of retries for keep alive messages.	1 to 10
NIF Group Name	The name of the Network Interface group on the GSX.	Up to 23 alphanumeric characters
IP InterfaceGroup Name	The name of the Network Interface group on the SBC Core device.	Up to 23 alphanumeric characters

Configure CDC for SBC Core Nodes

In this section:

- [Configure CDC for an SBC Core Node](#)
 - [Configure CDC for Legacy LI](#)
 - [Configure CDC for IMS](#)
 - [Configure CDC for PCSI LI](#)
 - [Configure CDC for PacketCable 2.0](#)
 - [Create Diameter Peer for SBC Nodes with PacketcableVTwo](#)
 - [Create Diameter Realm Routes for SBC Nodes with PacketcableVTwo](#)
- [Configuring CDC for SBC SWe on Cloud](#)
 - [Viewing Nodes](#)
 - [Node Level LI Statistics](#)
- [Configuring Mediation Server for SBCs](#)
- [Delete a Mediation Server Created for SBC Core](#)

This section covers configuring Call Data Channel (CDC) for SBC Core nodes on **Ribbon Application Management Platform (RAMP)**.

If any of the nodes are already configured, the new configuration replaces the existing configuration.

Prerequisites

- SBC Core nodes are registered with RAMP.
- The CALEA credentials are set for the SBC Core device registered on RAMP. Refer to [Register an SBC Core Device](#).

Start

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC**.
3. Click **SBCs** in the navigation pane.
4. Perform one of the following:
 - To configure all SBC Core nodes:
 - i. Click **SBCs** in the navigation pane.
 - ii. Select or enter the values. Refer to [Configure CDC for SBC Core Nodes](#).
 - iii. Click **Configure All SBCs**.
 - To configure all configured SBC Core nodes:
 - a. Click **SBCs** in the navigation pane.
 - b. Click **Configured**.
 - c. Select or enter the values. Refer to [Configure CDC for SBC Core Nodes](#).
 - d. Click **Configure All Configured SBCs**
5. To configure all non-configured SBC Core nodes:
 - a. Click **SBCs** in the navigation pane.
 - b. Click **Non Configured**.
 - c. Select or enter the values. Refer to [Configure CDC for SBC Core Nodes](#).
 - d. Click **Configure All Non Configured SBCs**
6. Click **Configure All SBCs**

Configure CDC parameters

Attribute	Description	Value Range
Interception Standard	The interception standard.	• 3gpp – 3rd Generation Partnership Project • etsi – European Telecommunication Standards Institute • packetcable (default) – PacketCable, the industry consortium founded by CableLabs. • packetcablePlusEtsi • packetcableVTwo

Attribute	Description	Value Range
Vendor ID	The ID of the vendor.	• none • ss8 • ultimaco • atos atos displays only if Interception Standard is set to "packetcableVTwo". • verint • groupTwoThousand SS8 displays only if Interception Standard is set to "packetcable".
Primary Mode	The operating mode of the Primary Intercept server. The parameter displays only when the following conditions are met: • The SBC personality is not media (M-SBC). • Interception Standard is any of the following: ◦ packetcable ◦ packetcablePlusEtsi • Vendor ID is any of the following: ◦ verint ◦ utimaco ◦ none	• Active • Standby • Out of Service

Attribute	Description	Value Range
Primary State	The state of the Primary Intercept server. The parameter displays only when the following conditions are met: • The SBC personality is not media (M-SBC). • Interception Standard is any of the following: ◦ packetcable ◦ packetcablePlusEtsi • Vendor ID is any of the following: ◦ verint ◦ utimaco ◦ none	• Enabled: Enables communication to the primary LI server. • Disabled: Disables communication to the primary LI server.
Secondary Mode	The operating mode of the Secondary Intercept Server. The parameter displays only when the following conditions are met: • The SBC personality is not media (M-SBC). • Interception Standard is any of the following: ◦ packetcable ◦ packetcablePlusEtsi • Vendor ID is any of the following: ◦ verint ◦ utimaco ◦ none	• Active • Standby • Out of Service
Secondary State	The state of the Secondary Intercept server. The parameter displays only when the following conditions are met: • The SBC personality is not media (M-SBC). • Interception Standard is any of the following: ◦ packetcable ◦ packetcablePlusEtsi • Vendor ID is any of the following: ◦ verint ◦ utimaco ◦ none	• Enabled: Enables communication to secondary LI Server. • Disabled: Disables communication to secondary the LI server.

Attribute	Description	Value Range
Primary IP	Enter the IP address of the Lawful Intercept device. The parameter displays only when the following conditions are met: • The SBC personality is not media (M-SBC). • Interception Standard is any of the following: ◦ packetcable ◦ packetcablePlusEtsi • Vendor ID is any of the following: ◦ verint ◦ utimaco ◦ none	A valid IPv4 address
UDP Port	UDP port on the mediation device. The Ribbon network element sends the call data to this UDP Port. The parameter displays only when the following conditions are met: • The SBC personality is not media (M-SBC). • Interception Standard is any of the following: ◦ packetcable ◦ packetcablePlusEtsi • Vendor ID is any of the following: ◦ verint ◦ utimaco ◦ none	0 to 65535
Secondary IP (optional)	Secondary IP address of the mediation device. The parameter displays only when the following conditions are met: • The SBC personality is not media (M-SBC). • Interception Standard is any of the following: ◦ packetcable ◦ packetcablePlusEtsi • Vendor ID is any of the following: ◦ verint ◦ utimaco ◦ none	A valid IPv4 address

Attribute	Description	Value Range
Keep Alive Timer	Interval for CDC keep alive messages from the Ribbon network element to the mediation device. The parameter displays only when the following conditions are met: • The SBC personality is not media (M-SBC). • Interception Standard is any of the following: ◦ packetcable ◦ packetcablePlusEtsi • Vendor ID is any of the following: ◦ verint ◦ utimaco ◦ none	0 to 65535
Keep Alive Retries	Number of retries for keep alive messages. The parameter displays only when the following conditions are met: • The SBC personality is not media (M-SBC). • Interception Standard is any of the following: ◦ packetcable ◦ packetcablePlusEtsi • Vendor ID is any of the following: ◦ verint ◦ utimaco ◦ none	1 to 10
Li Pol Dip For Regd Ood Msg	The parameter Li Pol Dip For Regd Ood Msg when enabled is used to indicate SBC to send policy request to PSX for registered Out-Of-Dialog requests(messages) to be intercepted. When this parameter is disabled, policy request is not sent to PSX for registered Out-Of-Dialog requests (messages). This field displays only when Interception Standard is "etsi" or "threeGpp".	• Enabled • Disabled

Attribute	Description	Value Range
RTCP Interception	Use this field to enable or disable Real-Time Control Protocol (RTCP) interception for the mediation server. This field displays only when either of the following conditions are met: • Interception Standard is "etsi" or "threeGpp" • Interception Standard is "packetcable" and Vendor ID is "ss8"	• Enabled • Disabled
Mediation Server Name	Enter a name for the mediation server. This field displays only when either of the following conditions are met: • Interception Standard is "etsi" or "threeGpp" • Interception Standard is "packetcable" and Vendor ID is "ss8"	
Interception Type	Select any of the following as Interception type. This field displays only when either of the following conditions are met: • Interception Standard is "etsi" or "threeGpp" • Interception Standard is "packetcable" and Vendor ID is "ss8"	• Media • Signaling: Signaling is supported only when the following conditions are met: ◦ Interception Standard is "etsi" or "threeGpp" ◦ Protocol Transport Type is "TCP".
Protocol Transport Type	The transport protocol type. This field displays only when either of the following conditions are met: • Interception Standard is "etsi" or "threeGpp" • Interception Standard is "packetcable" and Vendor ID is "ss8"	• TCP (default): Transmission Control Protocol • UDP: User Datagram Protocol
DSCP	Enter a value for Access Function application. This field displays only when either of the following conditions are met: • Interception Standard is "etsi" or "threeGpp" • Interception Standard is "packetcable" and Vendor ID is "ss8"	0 to 63 Default value: 32

Attribute	Description	Value Range
Operational State	Set the operation status of the link between the mediation server and RAMP. This field displays only when either of the following conditions are met: • Interception Standard is "etsi" or "threeGpp" • Interception Standard is "packetcable" and Vendor ID is "ss8"	• In-Service: The transport link is operational. • Out-of-Service: The transport link is not operational.
Administrative State	The Admin State. This field displays only when either of the following conditions are met: • Interception Standard is "etsi" or "threeGpp" • Interception Standard is "packetcable" and Vendor ID is "ss8"	• Enabled: Enables the connection between RAMP and the mediation server. • Disabled: Terminates the connection between RAMP and mediation server.
IP Address	Enter the IP address of the mediation device. The Ribbon network element sends the call data to this IP Address. The IP address of the port being used is included every call data message. The intercept server responds to these messages using the IP address received from the Ribbon network element. The Ribbon network element sends one message at a time to the intercept server. This field displays only when either of the following conditions are met: • Interception Standard is "etsi" or "threeGpp" • Interception Standard is "packetcable" and Vendor ID is "ss8"	A valid IPv4 or IPv6 address
Port	Enter the port on the mediation device. The Ribbon network element sends the call data to this port. This field displays only when either of the following conditions are met: • Interception Standard is "etsi" or "threeGpp" • Interception Standard is "packetcable" and Vendor ID is "ss8"	1 to 65535

Attribute	Description	Value Range
IP Interface Group Name	Enter the name of the Network Interface group on the SBC Core device to which the call data channel is associated.	Up to 23 characters
Media IP InterfaceGroup Name	Enter the name of the IP interface group used to stream media packets to the LI server. The parameter displays only if the SBC personality is not signaling (S-SBC).	Up to 23 characters
DSR Version	Enter the DSR (X2) Protocol Version value. This field displays only when Interception Standard is set as "etsi" or "threeGpp".	• 0 • 1

Configure CDC for an SBC Core Node

In this section:

- [Configure CDC for Legacy LI](#)
- [Configure CDC for IMS](#)
- [Configure CDC for PCSI LI](#)
- [Configure CDC for PacketCable 2.0](#)
 - [Create Diameter Peer for SBC Nodes with PacketcableVTwo](#)
 - [Create Diameter Realm Routes for SBC Nodes with PacketcableVTwo](#)

This section covers configuring Call Data Channel (CDC) for an SBC Core node.

Configure CDC for Legacy LI

This section covers configuring CDC for Legacy LI nodes SBC Core on Ribbon Application Management Platform (RAMP). If any nodes are already configured, the new configuration replaces the existing one.

Prerequisites

- SBC Core node is registered with RAMP.
- The CALEA credentials are set for the SBC Core device registered on RAMP. Refer to [Register an SBC Core Device](#).

Start

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC.**
3. Click **SBCs** in the navigation pane.
4. Click **Configured.**
5. Click on a node.
6. Select or enter the CDC parameters.
7. Click **Configure** <SBC node name>

CDC Parameters

Attribute	Description	Value
Gateway Name	Gateway name for the node.	
Network Element ID	The Network Element ID uniquely identifies each Ribbon network element. Network Element ID is generated and assigned by RAMP during the node registration process. The Network Element ID is included in the Call Data sent to the IS/MD. The IS/MD determines the origination point for the intercept the SBC. Configure the partner's mediation device separately to identify the assigned NE IDs, if necessary. The system includes the node number in every CDC message as per the PacketCable PKT-SP-EM- I08-040113 specification.	
Node Number	The global unique node number for the SBC used by the LI Server for ID.	
CDC Name	The name of the LI Call Data Control Channel configured by the user.	Up to 23 alphanumeric characters. The characters #%^&(){}<>,/\;`[]=!\$"*? ~ and SPACE are not allowed.
Interception Standard	The interception standard.	packetcable (default) – PacketCable, the industry consortium founded by CableLabs.
Vendor ID	The ID of the vendor.	• none
Primary Mode	The operating mode of the Mediation server for X2 signaling.	• Active • Standby • Out of Service

Attribute	Description	Value
Primary State	The state of the Primary Intercept server.	• Enabled: Enables communication to the primary LI server. • Disabled: Disables communication to the primary LI server.
Secondary Mode	The operating mode of the Secondary Intercept Server.	• Active • Standby • Out of Service
Secondary State	The state of the Secondary Intercept server.	• Enabled: Enables communication to secondary LI Server. • Disabled: Disables communication to secondary the LI server.
Primary IP	Enter the IP address of the Mediation server for X2 signaling.	A valid IPv4 address
UDP Port	UDP port on the mediation device. The Ribbon network element sends the call data to this UDP Port.	0 to 65535
Secondary IP (optional)	The secondary IP address of the mediation device.	A valid IPv4 address
Keep Alive Timer	Interval for CDC keep-alive messages from the Ribbon network element to the mediation device.	0 to 65535
Keep Alive Retries	Number of retries for keep-alive messages.	1 to 10
IP Interface Group Name	Enter the name of the IP interface Group to send the X2 messages.	Up to 23 characters
Media IP InterfaceGroup Name	Enter the name of the IP interface group used to stream media packets to the LI server.	Up to 23 characters

Configure CDC for IMS

This section covers configuring Call Data Channel (CDC) with IMS LI for an SBC Core node on Ribbon Application Management Platform (RAMP). If the nodes are already configured, the new configuration replaces the existing one.

Prerequisites

- The SBC Core node is registered with RAMP.
- The CALEA credentials are set for the SBC Core device registered on RAMP. Refer to [Register an SBC Core Device](#).

Start

Use this procedure to configure CDC for IMS:

1. Log on to the RAMP GUI as `calea` user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC**.
3. Click **SBCs** in the navigation pane.
4. Click **Configured**.
5. Click on a node.
6. Select the **Create Mediation Server** checkbox. Additional fields are displayed.
7. Select or enter the **CDC parameters**.
8. Click **Configure** <SBC node name>.

Note

Repeat steps 7 to 8 to add additional Mediation Servers. Up to 16 Mediation Servers are supported.

CDC Parameters

Attribute	Length/Range	Description
Gateway Name	N/A	Gateway name for the node. This field is auto-populated and not editable.
Network Element ID	N/A	The Network Element ID uniquely identifies each Ribbon network element. This field is auto-populated and not editable. Network Element ID is generated and assigned RAMP during the node registration process. The Network Element ID is in the Call Data sent to the IS/MD. The IS/MD determines the origination point to intercept the SBC. Configure the partner's mediation device separately to identify the assigned NE Ids, if necessary. The system includes the node number in every CDC message. The parameter is sent in the DSR messages.

Attribute	Length/Range	Description
Node Number	N/A	The global unique node number for the SBC used by the LI server for ID. This field is auto populated and cannot be edited.
CDC Name	Up to 23 alphanumeric characters.	The name of the LI Call Data Control Channel configured by the user. (Characters not allowed: #%^&(){}<>,/\;`[]=!\$"*? ~ and SPACE key)
Interception Standard	N/A	The interception standard to use. • 3gpp – 3rd Generation Partnership Project • ETSI - European Telecommunication Standards Institute
Vendor ID	N/A	The global unique node number for the SBC used by the LI Server for ID. You can choose the Vendor ID from the drop-down list. The Default value is none.
Li Pol Dip For Regd Ood Msg	N/A	Enable this flag to notify the SBC to send policy requests to the PSX for the registered Out-Of-Dialog requests (messages) to intercept. • Enabled • Disabled (Default)
RTCP Interception	N/A	Enable this flag for the Mediation Server to perform Real-Time Control Protocol (RTCP) interception. • Enabled • Disabled (Default)
DSR Version	N/A	Enter the DSR (X2) Message version value. • 0 (Default) • 1
IP InterfaceGroup Name	Up to 23 characters	Enter the name of the IP Interface group on the SBC Core device to initiate the X2 messages.
Media IP InterfaceGroup Name	Up to 23 characters	Enter the name of the Media IP Interface Group that streams media packets to the LI server.

Attribute	Length/Range	Description
Note When you use an invalid SIP Trunk Group (TG) name to configure IMS LI CDC, the SBC rejects the request, and the RAMP shows an error in the GUI. You must separate SIP TGs with commas (Do not use multiple commas in a row or other characters). You can configure supported or exempted SIP TGs.		
sipTrunkGroupSupportedList	Up to 4096 characters	List of Trunk Groups (TGs) marked for Lawful interception. For example: TG1,TG2,TG3.
sipTrunkGroupExemptedList	Up to 4096 characters	List of Trunk Groups (TGs) exempted from Lawful interception. For example: TG1,TG2,TG3.
Mediation Server		
Mediation Server Name	No character restrictions.	Enter a name for the Mediation Server.
Interception Type	N/A	The type of interception to use for this Media Server. • Media (Default) • Signaling
Protocol Transport Type	N/A	The IP transport type to use for media/signaling. • TCP – (Default) Transmission Control Protocol • TLS – Transport Layer Security • UDP – User Datagram Protocol Note UDP is not applicable for Signaling.
IP Address	N/A	Enter the IP address of the mediation device. The Ribbon network element sends the call data/call content to this IP Address. By default, the field is empty.
Port	1 to 65535	Enter the port on the mediation device. The Ribbon network element sends the call data/call content to this port.

Attribute	Length/Range	Description
DSCP	0 to 63	Enter a value for the DSCP for the X2/X3 packets. The default value is 32.
Operational State	N/A	Set the operation status of the link between the Mediation Server and RAMP. • In-Service: The transport link is operational. • Out-of-Service: (Default) The transport link is not operational.
Administrative State	N/A	The administrative state of this Mediation Server. • Enabled – Enables the connection between the SBC Core and the Mediation Server. • Disabled – (Default) Terminates the connection between RAMP and the Mediation Server.
DF Group Name	Supports up to 63 characters.	Use this optional field in the Mediation Server when • the Interception Type is set to "Signaling", • the Interception Standard is set to "3gpp" or "etsi," and • the Vendor ID is set to "verint," "groupTwoThousand," "utimaco" or "none." • After creating the Mediation Server, you can modify/remove the DF Group Name.
Keep Alive Time	0 to 65535	Interval for CDC keep-alive messages from the Ribbon network element to the mediation device. By default, the field is empty.
Keep Alive Interval	1 to 60	The keep-alive interval, in seconds, for signal generation. By default, the field is empty.
Keep Alive Probe	1 to 20	The maximum number of TCP keep-alive probes to send until the SBC decides that the connection is broken. By default, the field is empty.

Attribute	Length/Range	Description
TLS Profile Name	N/A	You can create multiple TLS Profiles on the SBC. A Calea user on RAMP can select any of these TLS Profiles in the Media Server configuration's TLS Profile Name attribute. You can modify the TLS profile after creating the Mediation Server. The default value is "defaultTlsProfile".

Configure CDC for PCSI LI

This section covers configuring CDC with P-Com.Session-Info (PCSI) for an SBC Core node on Ribbon Application Management Platform (RAMP). If the nodes is already configured, the new configuration replaces the existing configuration.

Prerequisites

- SBC Core node is registered with RAMP.
- The CALEA credentials are set for the SBC Core device registered on RAMP. Refer to [Register an SBC Core Device](#).

Start

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC**.
3. Click **SBCs** in the navigation pane.
4. Click **Configured**.
5. Click on a node.
6. Select the **Create Mediation Server** check-box. Additional fields appear.
7. Select or enter the CDC parameters.
8. Click **Configure** <SBC node name>.

Attribute	Description	Value
Gateway Name	Gateway name for the node.	

Attribute	Description	Value
Network Element ID	The Network Element ID uniquely identifies each Ribbon network element. Network Element ID is generated and assigned by the RAMP during the node registration process. The Network Element ID is included in the Call Data sent to the IS/MD. The IS/MD determines the origination point for the intercept the SBC. You need to configure the partner's mediation device separately to identify the assigned NE IDs, if necessary. The system includes the node number in every CDC message as per the PacketCable PKT-SP-EM- 108-040113 specification.	
Node Number	The global unique node number for the SBC used by the LI Server for ID.	
CDC Name	The name of the LI Call Data Control Channel configured by the user.	Up to 23 alphanumeric characters. The characters #%^&(){}<>./\;`[]=!\$"*? ~ and SPACE are not allowed.
Interception Standard	The interception standard.	packetcable (default) – PacketCable, the industry consortium founded by CableLabs.
Vendor ID	The ID of the vendor.	ss8
RTCP Interception	Enable or disable Real-Time Control Protocol (RTCP) interception for the mediation server.	- Enabled - Disabled
Media IP InterfaceGroup Name	Enter the name of the IP interface group used to stream media packets to the LI server.	Up to 23 characters
Mediation Server		
Mediation Server Name	Enter a name for the mediation server.	
Interception Type	Interception type.	Media
Protocol Transport Type	The transport protocol type.	TCP (Transmission Control Protocol)

Attribute	Description	Value
IP Address	Enter the IP address of the mediation device. The Ribbon network element sends the call content to this IP Address.	A valid IPv4 or IPv6 address
Port	Enter the port on the mediation device. The Ribbon network element sends the call content to this port.	1 to 65535
DSCP	Enter a value for Access Function application.	0 to 63 Default value: 32
Operational State	Set the operation status of the link between the mediation server and the SBC.	• In-Service: The transport link is operational. • Out-of-Service: The transport link is not operational.
Administrative State	The Admin State.	• Enabled: Enables the connection between RAMP and the mediation server. • Disabled: Terminates the connection between RAMP and mediation server.
Keep Alive Time	Interval for CDC keep alive messages from the Ribbon network element to the mediation device.	0 to 65535
Keep Alive Interval	The interval in seconds for keep alive signal generation in seconds.	1 to 60
Keep Alive Probe	The maximum number of TCP Keep-alive probes to send until SBC decides that the connection is broken.	1 to 20

Configure CDC for PacketCable 2.0

In this section:

- [Create Diameter Peer for SBC Nodes with PacketCableVTwo](#)
- [Create Diameter Realm Routes for SBC Nodes with PacketCableVTwo](#)

This section covers configuring CDC with PacketCable 2.0 for an SBC Core node on Ribbon Application Management Platform (RAMP). If the nodes are already configured, the new configuration replaces the existing configuration.

Prerequisites

- SBC Core node is registered with RAMP.
- The CALEA credentials are set for the SBC Core device registered on RAMP. Refer to [Register an SBC Core Device](#).
- The Diameter node is configured.

Start

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC**.
3. Click **SBCs** in the navigation pane.
4. Click **Configured**.
5. Click on a node.
6. Select the **Create Mediation Server** check-box. Additional fields appear.
7. Select or enter the CDC parameters.
8. Click **Configure** <SBC node name>.

Note

Repeat steps 7 to 9 to add up to 16 mediation servers.

CDC Parameters

Attribute	Description	Value
Gateway Name	Gateway name for the node.	
Network Element ID	The Network Element ID uniquely identifies each Ribbon network element. RAMP generates and assigns the Network Element ID during the node registration process. The Call Data sent to the IS/MD includes the Network Element ID. The IS/MD determines the origination point for the intercept (the SBC Core). Configure the partner's mediation device separately to identify the assigned NE IDs, if necessary. The system includes the node number in every CDC message as per the PacketCable PKT-SP-EM- I08-040113 specification.	
Node Number	The global unique node number for the SBC used by the LI Server for ID.	

Attribute	Description	Value
CDC Name	The name of the LI Call Data Control Channel configured by the user.	Up to 23 alphanumeric characters. The characters #%^&(){}<>./\;>[]=!\$"*? ~ and SPACE are not allowed.
Interception Standard	The interception standard.	packetcableVTwo packet cable version 2.0
Vendor ID	The vendor name of the LI server.	• none • atos
Li Pol Dip For Regd Ood Msg	Sets SBC Core to send policy request to PSX for registered Out-of-Dialog requests (messages) to be intercepted. When this parameter is disabled, policy request is not sent to the PSX for registered Out-of-Dialog requests (messages).	• Enabled • Disabled
RTCP Interception	Specifies whether to intercept Real-Time Control Protocol (RTCP) information for the mediation server.	• Enabled: SBC intercepts RTCP information • Disabled: SBC does not intercept RTCP information.
Diameter Node Name	Specifies the name assigned to the SBC Diameter node configuration. The SBC configuration includes a single Diameter node to define the SBC side of the Diameter interface. If Diameter is used for more than one purpose on the SBC then the Diameter node is shared. Note A user with admin privilege must complete Diameter node configuration. Using this parameter, a "calea" user enters the Diameter node name in the CDC for a PC 2.0 LI. The "calea" user creates additional Diameter objects within the CDC.	Up to 32 characters
Embed TapId In CccId	Sets whether to embed the tapId in the CCCID.	• Disabled (default) • Enabled

Attribute	Description	Value
IP Interface Group Name	The name of the Network Interface group on the SBC Core device to which the call data channel is associated.	Up to 23 characters
Media IP InterfaceGroup Name	The name of the IP interface group used to stream media packets to the LI server.	Up to 23 characters
Mediation Server		
Mediation Server Name	The name for the mediation server.	
Interception Type	Interception Type.	• Media • Signaling
Protocol Transport Type	The transport protocol type. Note The field displays only if the "Interception Type" is "Media".	UDP (User Datagram Protocol)
IP Address	Specifies the IP address of the mediation device. The Ribbon network element sends the call data to this IP Address. Every call data message includes the IP address of the port used. The intercept server responds to these messages using the IP address received from the Ribbon network element. The Ribbon network element sends one message at a time to the intercept server. Note The field displays only if the "Interception Type" is media.	A valid IPv4 or IPv6 address

Attribute	Description	Value
Port	The port on the mediation device. The Ribbon network element sends the call data to this port. Note The field displays only if the "Interception Type" is "Media".	1 to 65535
DSCP	The value for Access Function application. Note The field displays only if the "Interception Type" is "Media".	0 to 63 Default value: 32
Operational State	The operation status of the link between the mediation server and RAMP.	- In-Service: The transport link is operational. - Out-of-Service: The transport link is not operational.
Administrative State	The administrative status.	- Enabled: Enables the connection between RAMP and the mediation server. - Disabled: Terminates the connection between RAMP and mediation server.
Realm Name	The name of the realm in which the mediation server is configured. Note The field displays only if the "Interception Type" is "Signaling".	

Attribute	Description	Value
DF Group Name	The name of the DF group to which the call data of the target under surveillance is delivered. The DF Group name must correspond to the name of Delivery Function Server Group configured on the SBC Core node. Provision Delivery Function Server Group on the SBC core node prior to provisioning surveillances. Using the DF group name, the SBC Core node maps the Realm name for routing DIAMETER X2 traffic. Note The field displays only for SBC Core 10.0 and later versions with Interception Type as Signaling.	Up to 63 characters in the FQDN format

Create Diameter Peer for SBC Nodes with PacketcableVTwo

The X2 interface is an extension of the Diameter base protocol for event-based messaging using Diameter Accounting messages. The X2 Diameter-based interface supports sending intercepted Call Data (CD) and associated call events to the DF. This procedure covers creating a Diameter Peer for SBC Core devices on Ribbon Application Management Platform (RAMP).

Note

The procedure is applicable only for PacketcableVTwo.

Prerequisites

- SBC Core node is registered with RAMP.
- The CALEA credentials are set for the SBC Core device registered on RAMP. Refer to [Register an SBC Core Device](#).

Start

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC**.
3. Click **SBCs** in the navigation pane.
4. Create a Diameter Peer for all SBC nodes, or just one node, using a sub-step below:
 - To create Diameter Peer for all SBC nodes:
 - i. Click **Configured**.
 - ii. Click **Create Diameter Peer for All SBCs**.
The "Create Peer For All SBCs" dialog box displays.
 - iii. Proceed to step 5 to populate the dialog box fields.
 - To create Diameter Peer for a single SBC node:
 - i. Click **Configured**.
 - ii. Under the **Configured** tree, select an SBC node:

- iii. Click **Create Diameter Peer**.
The "Create New Peer" dialog box displays.
 - iv. Continue to step 5 to populate the dialog box fields.
5. Enter or select the values. For the values, refer to [Create Diameter Peer for SBC Nodes with PacketcableVTwo](#).
 6. Click **Create**.

Diameter Peer parameters

Parameter	Description	Value Range	Default Value	Mandatory (M)/ Optional (O)
CDC Name	The name of the LI Call Data Control Channel configured by the user.	Up to 32 alphanumeric characters. The characters #%^&(){}<>, \, ;, ` [] = ! \$ " ' ? ~ and SPACE are not allowed.		M
Diameter Peer Name	The logical name of the Diameter peer. Use unique names for Diameter peers under calea and admin users.	Up to 32 alphanumeric characters. The characters #%^&(){}<>, \, ;, ` [] = ! \$ " ' ? ~ and SPACE are not allowed.		M
State	The Admin state of the peer.	- enabled - disabled	disabled	M
IP Address	The optional IP address of the peer.	0 to 63		O
DSCP	The DSCP value for the peer.	0 to 63	16	
FQDN	The FQDN for the peer to use in the DNS query if the IP address is not configured.	Up to 256 characters		O
TCP Port	The TCP port number of the peer.	0 to 65535	3868	O
Device Watchdog Timer	The interval for the SBC to send Device-Watchdog-Requests.	0 to 100000 milliseconds	1000	O

Parameter	Description	Value Range	Default Value	Mandatory (M)/ Optional (O)
Device Watchdog Timer Answer Timeout	The timeout interval for the SBC to receive a Device-Watchdog-Answer from the peer for every Device-Watchdog-Request. If the peer does not send Device-Watchdog-Answer before the timeout expires, the SBC treats the peer as down.	50 to 500000 milliseconds	2000	O
Session Distribution	The order of distributing new sessions to multiple IP connections under the peer.	- honor-reply-order - round-robin	honor-reply-order	O

View Diameter Peers

To view Diameter Peers:

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC**.
3. Under the **CDC Devices** tree, click **SBCs**.
4. Click **Configured**.
5. Under the **Configured** tree, select an SBC node:
6. Click **View All Diameter Peers**.

The **View All Diameter Peers** pane displays.

Create Diameter Realm Routes for SBC Nodes with PacketcableVTwo

This procedure covers creating a create Realm Route for the SBC nodes on Ribbon Application Management Platform (RAMP)

Note

The procedure is applicable only for PacketcableVTwo.

Prerequisites

- SBC Core node is registered with RAMP.
- The CALEA credentials are set for the SBC Core device registered on RAMP. Refer to [Register an SBC Core Device](#).

Start

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC**.
3. Under the **CDC Devices** tree, click **SBCs**.
4. Create a Realm Route for all SBC nodes, or just one node, using a sub-step below:
 - To create Realm Route for all SBC nodes:
 - i. Click **Configured**.
 - ii. Click **Create Realm Route for All SBCs**.

- The "Create Realm Route for All SBCs" dialog box displays.
- iii. Proceed to step 5 to populate the dialog box fields.
 - To create Realm Route for an SBC node:
 - i. Click **Configured**.
 - ii. Under the **Configured** tree, select an SBC node:
 - iii. Click **Create Diameter Realm Route**.

The **Create New Realm Route** dialog box displays.

 - iv. Continue to step 5 to populate the dialog box fields.
 5. Enter or select the values. For the values, see [Realm Route parameters](#).
 6. Click **Create**.

Parameter	Description	Value Range	Default Value	Mandatory (D)/ Optional (O)
CDC Name	The name of the LI Call Data Control Channel configured by the user.	Up to 23 alphanumeric characters. The characters #%^&(){}<>,/,;`[]=!\$"*? ~ and SPACE are not allowed.		M
Diameter Realm Route Name	The logical name of this Diameter Realm Route. Use unique names for Diameter Realm Route under calea and admin users.	Up to 32 alphanumeric characters. The characters #%^&(){}<>,/,;`[]=!\$"*? ~ and SPACE are not allowed.		M
Diameter Peer Name	The logical name of the Diameter peer. Use unique names for Diameter peers under calea and admin users.	Up to 32 alphanumeric characters. The characters #%^&(){}<>,/,;`[]=!\$"*? ~ and SPACE are not allowed.		M
Priority	The priority of the Realm Route. A lower the number indicates higher priority.	0 to 100	0	O
Realm	The Realm (FQDN) for the route.	Up to 256 alphanumeric characters.		M
App Id	The application ID for the route.	• x2 • x1	x2	M
State	The Admin state of the route.	• enabled • disabled	disabled	M

View Diameter Routes

To view Realm Routes:

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC**.
3. Under the **CDC Devices** tree, click **SBCs**.
4. Click **Configured**.
5. Under the **Configured** tree, select an SBC node:
6. Click **View All Realm Routes**.
The **View All Realm Routes** pane displays.

Configuring CDC for SBC SWe on Cloud

In this section:

- [Viewing Nodes](#)
- [Node Level LI Statistics](#)

You can configure the Ribbon network elements and point them at the appropriate mediation devices for call data and call content delivery.

Configure the LI Call Data Channel on SBC SWe cloud nodes to support interception. For LI, configure the CDC using the CDC Configuration Manager through Ribbon Application Management Platform (RAMP).

Prerequisites

- A cloud SBC SWe instance is created.
- An [SBC SWe cluster](#) is created.

Start

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Cluster CDC**.
3. Select the SBC cluster.
4. Click **Launch CDC Configuration Manager**. The **SBC Configuration Manager** window displays. For more information, refer to [Configuring the SBC for Lawful Interception](#).
5. Log out from the RAMP GUI.
6. Log on to the RAMP GUI as the admin user.
7. Navigate to **Device Management > Cluster Management > Manage VNFs**.
8. Select the SBC SWe cluster with the configuration.
9. Under the **Configurations** tab, click **Activate Configuration**.

Viewing Nodes

The LI configuration is distributed to the newly added nodes in a cluster. The existing nodes takes the LI configuration after rebooting the existing nodes.

To view the nodes in the cluster:

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Cluster CDC**.
3. Click **View Nodes**. The nodes list in the cluster appears.

Node Level LI Statistics

Ribbon Application Management Platform (RAMP) queries the status information for all the mediation servers configured and displays this information on the UI. The SBC statistics related to LI against media SBC and S-SBC are available for viewing.

Note

Only the 'calea' user can view the LI statistics.

Use the following procedure to view the LI statistics.

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Cluster CDC**.
3. Select a cluster.
4. Click **View Nodes**. The nodes list in the cluster appears.
5. Select a node.
6. Click **Launch Node LI Stats**. The **SBC Configuration Manager** window appears.

Configuring Mediation Server for SBCs

The SBC in the network acts as an Integrated SBC (I-SBC) to provide peering between an IMS network and other peering networks. The mediation server provisions network elements to intercept. Network elements expose provisioning, call data, and call content interface towards the mediation server for legal interception.

The mediation servers connect to the SBC through X2 and X3 interfaces to obtain call data and call content.

Mediation Server is supported only for the following configurations:

- IMS
- PacketCable and SS8
- PacketCable 2.0

Up to 16 mediation servers are supported in CDC.

The following procedure covers configuring a mediation server for SBCs through Ribbon Application Management Platform (RAMP).

Start

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC**.
3. Expand **CDC Devices**.
4. Expand **SBCs**.
5. Click **Configured**.
6. Click on a node. The **Configure CDC Device** window appears.
7. Select the **Create Mediation Server** check-box. Additional fields appear.
8. Select or enter values. Refer to [Configure CDC for SBC Core Nodes](#).
9. Click **Configure** <the device name>.

Delete a Mediation Server Created for SBC Core

This section covers deleting a mediation server created for SBC Core nodes in Ribbon Application Management Platform (RAMP).

Prerequisites

The Operational State is "Out Of Service" and the Administrative State is "Disabled" for the mediation server.

Start

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Configure CDC**.
3. Expand **CDC Devices**.
4. Expand **Configured**.
5. Expand a gateway name.
6. Expand a mediation server.
7. Click on the mediation server properties.
8. Click **Delete Mediation Server**. A message appears, prompting you to confirm.
9. Click **OK**. The mediation server is deleted.

Managing Mediation Servers

In this section:

- [Create a Mediation Server](#)
- [Importing TLS Security Certificate to RAMP](#)

Managing mediation server is supported only in some customer-specific deployments.

Ribbon Application Management Platform (RAMP) supports establishing a transport connection towards the mediation server with or without Transport Layer Security (TLS). Additionally, **RAMP** supports Lawful Intercept (LI) target provisioning over the TLS to accommodate SS8 delivery function communication over this interface. **RAMP** accomplishes this by enabling CALEA Intercept Access Points (IAP) to support multiple (two instances) regionally-deployed SS8 Delivery Function systems.

Mediation servers interact with **RAMP** over the X1 interface to provision LI targets. These mediation servers are ADMF servers.

Note

If you remove the LI license from **RAMP**, you cannot use the Lawful Intercept feature.

Note

Before you remove the LI license, remove the mediation servers configured.

Create a Mediation Server

In this section:

- [Update a Mediation Server](#)
- [Disable a Mediation Server](#)
- [Delete a Mediation Server](#)

This section covers creating a mediation server for a customer specific deployment in Ribbon Application Management Platform (RAMP). This procedure may not be applicable for your deployment.

Prerequisites

- The SBC Core node is registered with **RAMP**.
- The CALEA credentials are set for the SBC Core device registered on RAMP. Refer to [Register an SBC Core Device](#).

Start

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Mediation Server**.
3. Click **Create**.
4. Select or enter values. Refer to [Create a Mediation Server](#). Click **Save**. The mediation server is added successfully.
5. Click **Enable** to activate the new mediation server. If the mediation server goes down, **RAMP** tries to connect to it six times. After six attempts, the mediation server is automatically disabled. You must manually enable the mediation server.

Mediation Server parameters

Attribute	Description
Mediation Server Name	Enter a name for the mediation server.
Mediation Server IP Address	Enter Mediation Server IP address in any of the following formats: • IPv4 • IPv6
Mediation Server Port	Mediation Server Port Number.
TLS	Set Transport Layer Security to any of the following: • Enabled Enables the TLS connection towards the mediation server. • Disabled Disables the TLS connection towards the mediation server.

Attribute	Description
Admin State	Admin State can be any of the following: - Enabled The connection between RAMP and the mediation server is enabled. - Disabled The connection between RAMP and the mediation server is disabled.
Operational State	The status of the link between the mediation server and RAMP . - In-Service The transport link is operational. - Out-of-Service The transport link is not operational.
DSCP	Enter Access Function application DSCP value. Range: 1 to 63 Default value: 32
Allow Bulk Audit	RAMP allows for bulk audits in the Mediation Server. - Enabled (Default) RAMP returns multiple targets (Maximum 255) in the Target Service List to the mediation server. The Ribbon LI solution supports a total of 5000 targets to be audited in the LI target table. - Disabled RAMP returns single target to the mediation server.
Select File	Certificate details and file path. Select File is enabled only if you set TLS to enabled.

Update a Mediation Server

1. Log on to the **RAMP** GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Mediation Server**.
3. Expand **Mediation Servers**.
4. Select a mediation server.
5. Click **Disable**. The Mediation server is disabled.
6. Modify the parameters. Refer to [Create a Mediation Server](#).
7. Click **Update**. The Mediation server parameters are updated.
8. Click **Enable** to activate mediation server.

Disable a Mediation Server

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Mediation Server**.
3. Expand **Mediation Servers**.
4. Select a mediation server.
5. Click **Disable**. The mediation server is disabled. A message *Mediation Server is disabled successfully* appears.

Delete a Mediation Server

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Mediation Server**.
3. Expand **Mediation Servers**.
4. Select a mediation server.
5. Click **Disable**. The mediation server is disabled. A message *Mediation server is disabled successfully* appears.
6. Click **Delete**. A message *Mediation Server is deleted successfully* appears.

Importing TLS Security Certificate to RAMP

Use the following procedure to copy the TLS security certificate (required if HTTPS) to Ribbon Application Management Platform (RAMP). After you upgrade and configure the GR, import the security certificate from the cinder volume path: `/opt/raid/configuration/liCertificates`, as it is not copied to RAMP after the upgrade.

Start

1. After the RAMP upgrade completes and the GR is configured, copy the certificate from the path `/opt/raid/configuration/liCertificates` to your desktop.
2. Log on to the RAMP GUI as "calea" user.
3. Navigate to **Observability > Lawful Intercept > Mediation Server**.
4. Select a mediation server.
5. Click **Disable**. The Mediation server is disabled.
6. Click **Browse** and import the security certificate from the desktop, which was copied.
7. Click **Enable** to activate the mediation server with the new security certificate. The Mediation server is activated.
The Operation State changes to 'In Service'.

Mediation Server parameters

Attribute	Description	Value range
Mediation Server Name	A name for the mediation server.	
Mediation Server IP Address	The mediation server IP address.	• IPv4 • IPv6 (default)

Attribute	Description	Value range
Mediation Server Port	The port number of the mediation server.	
TLS	The Transport Layer Security.	• Enabled Enables the TLS connection towards the mediation server. • Disabled Disables the TLS connection towards the mediation server.
Admin State	Admin State of the mediation server.	• Enabled The connection between RAMP and the mediation server is enabled. • Disabled The connection between RAMP and the mediation server is disabled.
Operational State	The status of the link between the mediation server and RAMP.	• In-Service The transport link is operational. • Out-of-Service The transport link is not operational.
DSCP	Access Function application string.	1 to 32 Default value: 32
Select File	Certificate details and file path. Note Select File is enabled only if you set TLS to enabled.	

Provisioning LI Targets

In this section:

- [Overview](#)

- [Provisioning Limitations](#)

Additional topics:

- [Target Provisioning Sequence](#)
 - [Set LI API on Intercept Server](#)
 - [IS Generation of LI API Messages to RAMP](#)
 - [IS Generation of LI API Messages to RAMP for Packet Cable 2.0](#)
 - [Forwarding Target Data to PSX](#)
- [Apply Restrictions on Lawful Intercept Targets](#)

Overview

Provisioning Lawful Interface (LI) targets on the Ribbon system involves sending data from the LI provisioning API and exchanging messages between the Intercept Server (IS) and Ribbon Application Management Platform (RAMP).

The IS can use the LI Provisioning API to create, retrieve, update, and delete specific Lawful Intercept targets, and to retrieve a list all Lawful Intercept targets.

Note

The `ingressCalltoWirelessSub` parameter is read-only.

You can specify the LI target by these Intercept Criteria: Directory number, MSISDN/MDN, IMSI, IMEI, ESN, Business Group and Private VPN number, Authcode, SIP URI, Billing number.

Note

Only Directory Numbers (Called, Calling, or translated) and SIP URI are supported as LI criteria.

You can specify the interception Type: `Pen_and_Trap` (Calling party Pen Register data and Called party Trap and Trace data) only, or Title III Intercept with call data and content.

You can also specify:

- whether to intercept forwarded calls, and
- whether the provisioned intercept target is enabled.

Note

Ribbon systems perform a Title III intercept and send calling party data, called party data, and call content (when available and as directed) to the IS, which is responsible to deliver only what a warrant requires (Title III, Pen Register, or Trap and Trace) to the Law Enforcement Agency.

The Lawful-Intercept Identifier (LIID), or TAP-ID, identifier is assigned to every target configured using the X1 interface. In the mediation server, each TAP-ID uniquely identifies a single target record that is added by the ADMF server.

RAMP propagates each target's TAP-ID to the PSX and SBC Core systems for further processing.

RAMP does not support auditing the target information based on TAP-ID.

Provisioning Limitations

- Wildcards are supported for the target. An asterisk (*) is used as a wildcard indicator in the INTERCEPT_CRITERIA2_ID (for Type DN) or INTERCEPT_CRITERIA1_ID (for type SIP_URI) of the X1 interface messages. RAMP does not validate the Intercept criteria numbers.
- RAMP adds TAP-ID to all the X1 messages CREATE and UPDATE as an optional parameter.
- The valid range for the TAP-ID is between 1 and 2147483647 (4 bytes).
- TAP-ID is an optional field. If the target is created without a TAP-ID, then on retrieving it, RAMP does not send the TAP-ID in the response. The default value "0" is stored only on the PSX. This is to make RAMP compatible with existing clients who do not have TAP-ID.
- If the TAP-ID is not set for a target, RAMP does not add TAP-ID in the response of Retrieve and List requests.
- The DF Group Name (dfGroupName) is an optional field and supports up to 63 characters.

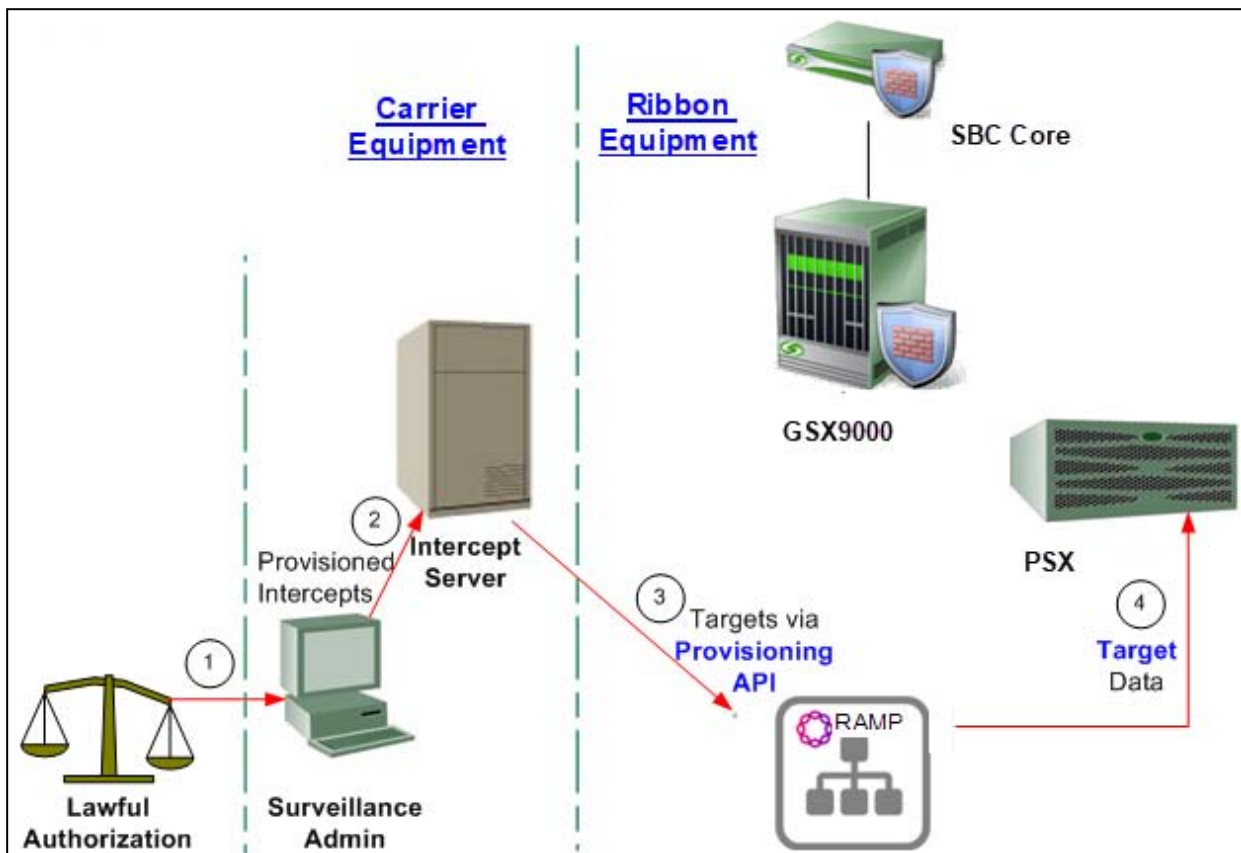
Target Provisioning Sequence

In this section:

- [Set LI API on Intercept Server](#)
- [Forwarding Target Data to PSX](#)

After the LI functionality establishes on the Ribbon equipment, and the IS communicates with Ribbon Application Management Platform (RAMP), provisioning of intercept targets follows the basic sequence shown in the figure below.

Lawful Intercept Provisioning



1. Lawful Intercept target provisioning data is entered into the IS through the partner's Surveillance Administration System. This procedure may be performed manually or through electronic provisioning, as determined by the carrier and law enforcement agencies.
2. For each intercept target, the IS generates a message over the SOAP-based API over TCP/IP to RAMP, specifying the intercept criteria.
3. RAMP processes the intercept criteria based upon the configured LI target settings (refer to [Apply Restrictions on Lawful Intercept Targets](#)) and replies to the IS with a message indicating success/failure of target provisioning.
4. RAMP distributes the target data to all primary PSX devices through the existing PIPE protocol.

The procedure to implement a Lawful Surveillance Intercept is as follows:

1. A court order is delivered to the service provider and the law enforcement agency identifying a targeted DN and authorizing it for pen register (egress call data), trap and trace (ingress call data), or Title III (call data and content) surveillance.
2. The service provider provisions the authorized surveillance on the appropriate network elements (in this case, on the PSX through RAMP that serve the targeted DN. This allows call data to be captured and delivered to the LEA. At the LEA, a collection function is provisioned to receive the data.
3. As calls are placed to/from the targeted DN, the switches (the SBC and GSX) retrieve the surveillance authorization from the PSX and capture the authorized data and deliver it to the IS, which passes it to the collection function at the LEA.
4. When surveillance authorization expires, the targeted DN is re-provisioned and the switches no longer capture call data.

Set LI API on Intercept Server

In this section:

- [IS Generation of LI API Messages to RAMP](#)
- [IS Generation of LI API Messages to RAMP for Packet Cable 2.0](#)

The Intercept Server sends LI provisioning data to **Ribbon Application Management Platform (RAMP)** via the LI API. The carrier must provide the following:

- The LI provisioning human interface and link to government servers on the Intercept Server.
- The functionality necessary for the Intercept Server to generate LI API messages.

The carrier must also configure the Intercept Server with the following information:

- The IP address and port on **RAMP** to send the API messages.
- **RAMP** LI administrator login and password, for inclusion in the header of API messages.

For details of the Ribbon LI API, including the WSDL defining the interface messages, refer to the Ribbon Lawful Intercept Interface Specification. To obtain the specification document, contact the Ribbon Global Support (GPS).

IS Generation of LI API Messages to RAMP

The API used to provision LI targets on the **Ribbon** equipment uses standard SOAP syntax (XML over HTTP) with the added **Ribbon**-specific definitions provided by a web services definition language (WSDL) file.

It is the service provider's responsibility to implement the LI API functionality at the Intercept Server.

Every SOAP message contains a valid user and password of the **Ribbon Application Management Platform (RAMP)** Lawful Intercept administrator, in the SOAP header to authenticate and authorize the received the API message.

Lawful Interception Operating System (LIOS) can replicate X2/X3 streams to different law enforcement agencies (LEAs), duplicate targets with different tap IDs are provisioned. Two operations "retrieveLawfulInterceptTargetV2" and "deleteLawfulInterceptTargetV2" takes the complex type "LawfulInterceptTargetKeys" as the input. The following complex type is available in Web Services Description Language (WSDL):

```
<complexType name="LawfulInterceptTargetKeys">
  <sequence>
    <element type="tns:interceptCriteriaTypeEnum" name="interceptCriteriaType"/>
    <element type="xsd:string" name="interceptCriteriaId"/>
    <element type="xsd:int" name="tapId"/>
  </sequence>
</complexType>
```

The IS/MD sends API messages to **RAMP** to perform the following operations:

- Create a Lawful Intercept target
- Retrieve a Lawful Intercept target
- Update a Lawful Intercept target
- Delete a Lawful Intercept target
- List all provisioned Lawful Intercept targets

Lawful Intercept Provisioning

Column name	Data type	NULL ?	Description
INTERCEPT_CRITERIA_TYPE	NUMBER (3)	No	Set Lawful Intercept target to any of the following: • 1 = DirectoryNo • 2 = MSISDN_MDN • 3 = IMSI • 4 = ESN • 5 = BusinessGroup_PrivateVPNNum • 6 = Authcode • 7 = SIP_URI • 8 = BillingNum Note Only Directory Numbers (Called, Calling, or translated) and SIP URI are supported as LI criteria.
INTERCEPT_CRITERIA_1_ID	VARCHAR(128)	No	Part 1 of Intercept criteria. The value is based on Intercept type as follows: • CountryId for Intercept types 1,2,3,8 • Electronic Seq Number for Intercept type 4 • Business Group Id for Intercept type 5 • AuthcodeId for Intercept type 6 • SIP URI for Intercept type 7
INTERCEPT_CRITERIA_2_ID	VARCHAR(64)	No	Part 2 of Intercept criteria. The value is based on Intercept type as follows: • NationalId for Intercept types 1,2,3,8 • Sonus_NULL for Intercept types 4,6,7 • VPN for Intercept type 5
INTERCEPTION_TYPE	NUMBER (3)	Yes	Type of Interception Read-only field. PSX can only allow provisioning. • 1 = PEN_AND_TRAP • 2 = INTERCEPT
FORWARDED_CALL_INTERCEPT	NUMBER (3)	Yes	Indicates if the forwarded call should be intercepted or not • 1 = A forwarded call should be intercepted. • 2 = A forwarded call should NOT be intercepted.

Column name	Data type	NULL ?	Description
INGRESS_CALL_WIRELESS_SUB	NUMBER (3)	Yes	This parameter (when set to true) is used to disable Ingress calls to wireless subs from being tapped unless they are forwarded at the GMSC (call delivery calls can continue to be intercepted at the Traffic MSC).
ENABLED	NUMBER (3)	Yes	Indicates if intercept criteria is enabled • 1 = Intercept Enabled for this target (Default). • 2 = Intercept Not Enabled for this target.
DATA	VARCHAR(3)	No	This parameter stores the Initialization Vector (IV). The IV is computed for each row of LI data using the INTERCEPT_CRITERIA1_ID and INTERCEPT_CRITERIA2_ID parameters.

For every Lawful Intercept target, specify the intercept type. The Ribbon equipment treats all intercepts as Title III (call data and content), and only reverts to Pen and Trap (data only) if no GSX or SBC device is available.

IS Generation of LI API Messages to RAMP for Packet Cable 2.0

In this section:

- [Lawful Intercept Deployment](#)
- [SOAP API Message Provisioning Behavior](#)
 - [X1 Message Structure](#)
 - [AddSurveillance](#)
 - [ModifySurveillance](#)
 - [RemoveSurveillance](#)
 - [RemoveAllSurveillance](#)
 - [GetSurveillance](#)
 - [GetAllSurveillance](#)
 - [Error Handling](#)

Ribbon LI supports PacketCable 2.0 for Q-SBC. Ribbon Application Management Platform (RAMP). RAMP supports the X1 interface-equivalent to the Q-SBC. The X1 interface towards the ADMF server for intercept provisioning is supported using SOAP API.

Lawful Intercept Deployment

- The SBC Core is deployed in Active-standby mode with **RAMP** and the external PSX.
- **RAMP** supports multiple CALEA users and ADMF (LI Administration Function) servers.
- The ADMF servers operate independently to configure the targets interfacing to **RAMP** using X1 over SOAP (HTTPS).

Note

When multiple ADMF servers are supported, TapID is unique across the mediation servers.

- Multiple DF2 servers connect to the SBC Core using Diameter (over optional IPsec).
- Multiple DF2 servers connect to the SBC Core using UDP (over optional IPsec).

RAMP accepts encrypted connections using TLS (with self-generated or external certificates) from any mediation server with valid credentials.

SOAP API Message Provisioning Behavior

SOAP API message provisioning behavior is described below:

- SOAP authentication is performed using the credentials of a dedicated CALEA user.
- Auditing and pagination is performed using TapID. TapID is the key for all operations.
- RAMP uses a different WSDL for PC 2.0 and old LI flavors. RAMP differentiates WSDL services using different URLs.
- RAMP secures the X1 interface using HTTPS. The TLS certificates are self-signed and locally generated or CA signed certificates.

The TLS 1.0 authentication patterns are listed below:

Ciphersuite	Key Exchange Method	Server Authentication Method	Encryption Algorithm (key size)	Message Authentication Hash
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	RSA	AES(128) CBC mode	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE	RSA	AES(128) CBC mode	SHA-1

X1 Message Structure

A surveillance provisioned via the SOAP based X1 interface consists of basic surveillance information. Use the following commands on RAMP for provisioning the PSX using the WSDL:

The WSDL defines two basic requests:

- `editConfig`: Add, modify, or delete surveillance provisioning
- `getConfig`: Retrieve a provisioned surveillance

Within the `editConfig` request, use the following commands to specify a command type:

- `addSurveillance`: Add a surveillance
- `modifySurveillance`: Modify a surveillance
- `removeSurveillance`: Delete a surveillance
- `removeAllSurveillance`: Delete all surveillance defined by a DF user

Within the `getConfig` request, use the following commands based on the filtering supplied in the request:

- `getSurveillance`: Retrieve a provisioned surveillance

The getConfig request option is indicated by the presence of a “tapId” block within the getConfig request.

- *getAllSurveillance*: Retrieve all surveillance provisioned by a DF user

Every request must contain the credentials block with the CALEA user details shared with the ADMF server.

AddSurveillance

The *AddSurveillance* command adds a surveillance record similar to *CreateLawfulInterceptTargetRequest*. **RAMP** sends create request to the PSX.

For more information on the commands, refer to Ribbon SBC Lawful Intercept Interface Specification for Packetcable 2.0.

The following parameters are used in this command.

Parameter	Description	Value range	Mandatory (M)/ Optional (O)
deviceName	The host name of RAMP .	string	M
pni	The parameter determines whether to intercept Call Content involving a target behind private or obscure network. If pni is set to True, the following parameters are mandatory: • Target Transmit Call Content DF Address • Target Transmit Call Content DF Port • Target Receive Call Content DF Address • Target Receive Call Content Port If pni is set to false, only the call data is intercepted.	boolean (True/False)	O

Parameter	Description	Value range	Mandatory (M)/ Optional (O)
txCcDfName	An optional string if Call Content is required for the target. The value is an IP address of the DF to which call content transmitted by the target is sent. If the parameter <i>txCcDfName</i> is set to true, the following parameters are mandatory: • Transmit CC DF Port • Receive CC DF Address/Port	IPv4/v6 address (string)	O
txCcDfPort	The port of the DF to which the call content transmitted by the target under surveillance is delivered. If the parameter <i>txCcDfPort</i> is set to true, the following parameters are mandatory: • Transmit CC DF Address • Receive CC DF Address/Port fields	standard port number 1 to 65535	O
rxCcDfName	An optional string if Call Content is required for the target. The value is an IP address of the DF to which call content received by the target is sent. If the parameter <i>rxCcDfName</i> is set to true, the following parameters are mandatory: • Transmit CC DF Address/Port • Receive CC DF Port	IPv4/v6 address (string)	O
rxCcDfPort	The port of the DF to which the call content received by the target under surveillance is delivered. If the parameter <i>rxCcDfPort</i> is set to true, the following parameters are mandatory: • Transmit CC DF Address/Port • Receive CC DF Address	standard port number 1 to 65535	O

Parameter	Description	Value range	Mandatory (M)/ Optional (O)
targetId	A string identifying the user agent under surveillance in the format of a username and host portion of a SIP URI or a DN (Directory Number) in a SIP or TEL URI. For example, username@domain, "6034565555" It must correspond to at least one of the possible contents of a SIP (or TEL) URI representing the surveillance target for calls/ signaling traversing the SBC.	string up to 255 characters	M
cdDfGroupName	The name of the DF group to which the call data pertaining to the target under surveillance is delivered.	string in FQDN format up to 63 characters	M
tapId	An alphanumeric string that uniquely identifies the surveillance. If the tapId is embedded in the CCCID (for X3), the acceptable range for tapId is a decimal value between 1 and 65534 as the tapId is embedded in 2 bytes out of the 4 bytes of CCCID. • If the tapId is null, it is converted to 0. • If the tapId is a decimal value in the range of 1 to 65534 (if the TapID is not a decimal number or out of range), it is converted to 65535 or hex 0xFFFF. The hexadecimal equivalent of the decimal value passed forms the two most significant bytes of the generated CCCID. If TapID is not embedded in CCCID, it is an alphanumeric string.	string up to 255 characters	M

Parameter	Description	Value range	Mandatory (M)/ Optional (O)
errorOption	The errorOption field is applicable only to editConfig requests with more than one surveillanceConfig block (in a single request message). If the errorOption field is not populated, the errorOption is set to “stop-on-error” by default. If an editConfig request contains a single surveillanceConfig block, the value of the errorOption field has no impact on the behavior of the request processing. • “ignore-error” ◦ If an error is encountered while processing multiple surveillanceConfig blocks (within a single editConfig request), then that error is noted, and processing continues with the next surveillanceConfig block. ◦ The response contains the errorTag value of “Partial Operation” and the error information corresponding to the first error that occurred. • “stop-on-error” ◦ If an error is encountered while processing multiple surveillanceConfig blocks (within a single editConfig request), the error is returned in the response and subsequent surveillanceConfig block are not processed.	Not used: Use of multiple surveillanceConfig blocks within a single editConfig request is not supported. The field is ignored as RAMP supports only one command per request.	O
credential	Every X1 SOAP request must contain an authentication block that contains user credentials (userid and password).	block	M
user	The userid, a member of the “calea” user group on RAMP.	string	M

Parameter	Description	Value range	Mandatory (M)/ Optional (O)
Password	The password of the calea user.	string	M

The IP address in txCcDfName and rxCcDfName supports IPv4 and IPv6 addresses.

The LI flavor treats the tapID along with the TargetID as the primary key. Multiple records are not added with the same tapID. Multiple records are not added for the same TargetID. Multiple ADMF servers require unique TapIDs.

ModifySurveillance

The *ModifySurveillance* command modifies the surveillance.

The `ModifySurveillance` command takes the same inputs as `AddSurveillance` identical processing. See [AddSurveillance](#).

RemoveSurveillance

The *removeSurveillance* command deletes a surveillance.

RAMP accepts the following parameters in the `removeSurveillance` command:

- `deviceName` : If the deviceName received does not match the SBC or the RAMP host name, the command is rejected.
- `tapID` : RAMP passes this info to PSX to fetch and delete from the database.

The command fails if the target record is not found with the tapID.

RemoveAllSurveillance

RAMP accepts the following parameters in the `removeAllSurveillance` command:

- `deviceName`: If the deviceName received does not match the SBC or RAMP host name, the command is rejected.

RAMP triggers the PSX to delete all the surveillance added (`addSurveillance`) by the DF user. The PSX deletes all the records that match the DF_USER.

The `removeAllSurveillance` command deletes all surveillance created by a specific DF user. Surveillance added by other DF users are not affected.

GetSurveillance

The *getSurveillance* command retrieves a single surveillance.

RAMP accepts the following parameters in the `getSurveillance` command:

- `deviceName` : If the deviceName received does not match the RAMP host name, the command is rejected.
- `tapID` : RAMP passes this info to the PSX to fetch from the database.

RAMP fetches the surveillance data from the PSX and sends the X1 response.

The response includes the following information:

- `deviceName`
- `pni`
- `cdDfGroupName`
- `txCcDfName`
- `txCcDfPort`
- `rxCcDfName`
- `rxCcDfPort`
- `targetID`
- `tapID`

GetAllSurveillance

The `getAllSurveillance` command retrieves multiple surveillance activities.

Only the surveillance added by the DF user specified in the `getConfig` request are retrieved. Any surveillance added by different DF users are not retrieved.

The control of the paged response message content is performed using of the following optional `getSurveillanceConfig` request attributes:

- `pageSize`: default value = 100, maximum value = 1000
- `pageIndex`: default value = 1

Surveillances contained in the `getAllSurveillance` response are ordered by `tapID`.

One `getAllSurveillance` request message results in only one response message (one page). If the number of surveillance provisioned by the DF user exceeds the count supported in one page, the DF is executed in a sequence of request/response messages in which the specified `pageIndex` value is incremented by one in every subsequent request. The DF can retrieve sequential pages of provisioned surveillance (ordered by `tapID`).

The combination of `pageSize` and `pageIndex` represents an absolute index to the surveillance table (filtered by `dfuser` and ordered by `tapID`). Separate request/response transactions are required to retrieve each page of surveillance.

RAMP accepts the following parameters in the `getAllSurveillance` command:

- `deviceName` : If the `deviceName` received does not match RAMP host name, the command is rejected.
- `pageIndex` : Page index indicates the current page to retrieve in which the surveillance are sorted based on `tapID` and partitioned into pages based on the `pageSize`.
- `pageSize` : Page size indicates the count of records that are required in the next response.

RAMP supports up to 1000 records per page

RAMP fetches the surveillance data from the PSX and sends the X1 response with all the records information bundled in a single response.

Error Handling

An X1 request in incorrect format results in a basic SOAP validation error.

Application errors include the following details.

- `errorTtype`: The field is always set to "application".

- **errorTag:** The errorTag field is populated with a value from the ErrorTag enumerated type defined in the error.xsd file. The ErrorTag value that is populated in the errorTag field is the error condition that closely aligns with the actual error.
- **errorSeverit:** This field is always set to “error”.
- **errorNumber:** The errorNumber field is populated with an integer that represents the actual error condition. The errorNumber has a 1:1 mapping with the text string that is displayed in the errorMessage field.
- **errorMessage:** Description of the actual error condition. Each string used in this field has a corresponding unique integer value which is displayed in the errorNumber field.

errorNumber	errorMessage	errorTag	Description
1	Badly formed request	OPERATION_FAILURE	The SOAP request is malformed.
2	Invalid user credentials	ACCESS_DENIED	The user credentials are not in the correct format.
3	Userid is not a member of the dfuser group	ACCESS_DENIED	The user ID is not of CALEA.
4	Internal credential validation error	OPERATION_FAILURE	The user authentication failed.
5	Internal Error	OPERATION_FAILURE	Any other internal error.
6	Missing SurveillanceConfig block	MISSING_ATTRIBUTE	NA
7	Missing SurveillanceConfig command	MISSING_ATTRIBUTE	NA
8	Missing SurveillanceConfig surveillance data	MISSING_ATTRIBUTE	NA
9	Missing device name	MISSING_ATTRIBUTE	The device name is missing.
10	Invalid device name	INVALID_VALUE	The device name does not match the RAMP host name.
11	Missing DfUser	MISSING_ATTRIBUTE	The username is missing.
12	Invalid PNI	INVALID_VALUE	The PNI value not Boolean.

errorNumber	errorMessage	errorTag	Description
13	Invalid TxCcAddress	INVALID_VALUE	The address is not in valid IP format.
14	Invalid RxCcAddress	INVALID_VALUE	The address is not in valid IP format.
15	Invalid TxCcPort	INVALID_VALUE	The port number is not in valid format.
16	Invalid RxCcPort	INVALID_VALUE	The port number is not in valid format.
17	Missing TxCcAddress	MISSING_ATTRIBUTE	The X3 Tx IP address is missing when PNI=true.
18	Missing RxCcAddress	MISSING_ATTRIBUTE	The X3 Rx IP address is missing when PNI=true.
19	Missing TxCcPort	MISSING_ATTRIBUTE	The X3 Tx port is missing when PNI=true.
20	Missing RxCcPort	MISSING_ATTRIBUTE	The X3 Rx port is missing when PNI=true.
21	Tap ID too long	INVALID_VALUE	Invalid TapID.
22	Invalid Tap ID	INVALID_VALUE	invalid TapID.
23	Missing Tap ID	MISSING_ATTRIBUTE	NA as tapID missing and treated as zero.
24	Tap ID already exists	DATA_EXISTS	Duplicate record insertion error.
25	Tap ID with given DfUser does not exist	OPERATION_FAILURE	Audit failure as the record was not created by the same user.
26	Invalid Target ID	INVALID_VALUE	Invalid targetID.
27	Missing Target ID	MISSING_ATTRIBUTE	targetID is missing.

errorNumber	errorMessage	errorTag	Description
28	Invalid Call Data DF Group Name	INVALID_VALUE	Cannot validate in RAMP.
29	Missing Call Data DF Group Name	MISSING_ATTRIBUTE	CDFGroup name is missing.
30	Invalid pageIndex	INVALID_VALUE	Audit page index out of bounds.
31	Invalid pageSize	INVALID_VALUE	Audit page size > 1000.
32	DB Insertion Error	OPERATION_FAILED	Add operation failed.
33	DB Modification Error	OPERATION_FAILED	Modify operation failed.
34	DB Remove Error	OPERATION_FAILED	Remove operation failed.
35	DB RemoveAll Error	OPERATION_FAILED	Remove all operation failed.
36	DB Get Error	OPERATION_FAILED	Audit failure.
37	DB Get ALL Error	OPERATION_FAILED	Audit failure without tapID.

Forwarding Target Data to PSX

When Ribbon Application Management Platform (RAMP) receives a provisioning message from the LI API, it converts the message data, as needed, and forwards it to every primary PSX for provisioning. RAMP automatically provisions one or many primary PSXs in the network.

Every primary PSX automatically creates, deletes, updates, or lists the specified LI_Target entities received from RAMP. However, there is no PSX GUI to provision or read LI content.

The provisioned LI criteria are compared with call data received in each Policy Request from an SBC Core device, or derived during call processing by the PSX. If there is a match, the PSX returns the matching LI criteria in the Policy Response.

Info

The default LI X2 messages has no information element to communicate the TapID to the Mediation Server.

Apply Restrictions on Lawful Intercept Targets

You can add restrictions on lawful Intercept targets in Ribbon Application Management Platform (RAMP).

RAMP allows you set the following:

- Restrict access to LI targets only for existing subscribers. Only the existing subscribers are designated as intercept targets.
 - Restrict access to LI targets only for the target owners (the user who created the target). A CALEA user can access only the LI targets created by that user. A user cannot access LI targets created by other users.
 - Send an error message if an operator attempts to delete an LI target (subscriber) that does not exist in the PSX database.
1. Log on to the RAMP GUI as "calea" user.
 2. Navigate to **Observability > Lawful Intercept > LI Target Settings**.
 3. Select or clear the checkboxes.
 4. Click **Apply**.

Check box	Description
Allow Lawful Intercept Targets for existing subscribers only	Restrict LI targets to existing subscribers only. Before creating an LI target, the PSX validates the subscriber DN in the database and returns an error if the DN is not found. When a Subscriber DN is deleted, the PSX removes all LI information from the database before deleting the DN. This option is not enabled by default. Note If you dynamically add a Softswitch entry to the PSX database, you must re-provision the “Allow Lawful Intercept Targets for existing subscribers only” setting.
Return an error when attempting to delete a non-existent LI target	Generate an error message through the RibbonLI API when the PSX attempts to delete an LI target that does not exist in the database. This option is disabled by default.

Check box	Description
Restrict access of LI targets by other CALEA users	Restrict access to LI targets created by other CALEA users. The restriction does not apply to existing targets, only applicable for the targets created after enabling the restriction. If you enable this restriction before deleting the targets and creating them again, the list and retrieve operation will not fetch the existing targets which do not contain the username stored in the PSX database. RAMP sends the username to the PSX only if the flag "Restrict access of LI targets by other CALEA users" is enabled. This option is disabled by default.

Call Processing

Contents

- [Call Data Interface](#)
 - [Call Data Channel Establishment](#)
 - [Call Data Messages](#)
- [Call Content Interface](#)
- [GSX Lawful Intercept Basic Call Processing](#)
- [SBC Lawful Intercept Basic Call Processing](#)

This section describes the processing of calls that meet the provisioned LI criteria, including the information sent from the PSX to the GSX in the routing response, the Call Data Interface messages exchanged between the GSX and the IS, and the Call Content streams delivered to a specified server. It contains the following sections:

- [Call Data Interface](#) describes the functionality of the Call Data interface used to transmit call progress messages from the GSX and SBC to the Intercept Server.
- [Call Content Interface](#) describes the RTP mechanism by which the GSX and SBC Core forward the voice content.
- [SBC Lawful Intercept Basic Call Processing](#) provides an example of interception of a call received by the SBC.

Call Data Interface

In this section:

- [Call Data Channel Establishment](#)
- [Call Data Messages](#)

When an LI call is in progress, the SBC and GSX send call progress information to the Intercept Server over the Call Data interface. This interface uses Radius over a UDP connection with a protocol based on the CableLabs

PKT-SP-EM- I08-040113 PacketCable Event Messages Specification, but with Ribbon-specific attributes and event messages added. Refer to the Ribbon **Lawful Intercept Interface Specification** for more information.

Call Data Channel Establishment

The GSX and SBC Core platforms include the following behavior when establishing Call Data Channels (CDCs) to the Intercept Server (IS):

- The GSX/SBC establishes a CDC over UDP/IP to the IS for sending call data of all intercepted calls to the IS. The GSX and SBC also send messages to the IS over this channel.
- The user configures the GSX/SBC with the UDP/IP address of the IS; refer to [Configuring Call Data Channel](#) for more information. The GSX/SBC periodically sends keep-alive messages to the IS to ensure it is reachable.
- The GSX/SBC includes the local IP address in the Radius NAS-IP-Address in the messages it sends to the IS. The IS uses this IP address to send a response to the GSX/SBC to avoid configuring the Ribbon platform's address information in the IS.

The GSX use both ports on the active MNS card and supports a switchover to the standby MNS card. The GSX first attempts to use the primary call data channel, if enabled. After a configurable number of retries is reached without an acknowledgment, the GSX attempts to use the secondary CDC, if enabled. This process repeats until an acknowledgment is received. Upon an MNS switchover, the GSX maintains the state of the CDC and continues in that state. The sequence number is reset after an MNS switchover.

Call Data Messages

In this section:

- [Startup and Keepalive](#)
- [Call Data Message Types](#)
- [Indication Messages](#)

When the policy response from the PSX indicates that an interception is needed, the GSX or SBC formats and sends call data messages to the Intercept Server for many stages of call processing.

The GSX or SBC expects to receive an ACK for each of the Packet Cable Event messages sent to the Intercept Server (IS). The IS re-transmits a message based on configuration and issues traps if the maximum number of re-transmissions is reached. The GSX or SBC transmits the next message to the IS only when receiving an ACK for the previously transmitted message.

Startup and Keepalive

Upon reboot, the GSX or SBC Core sends restart messages to the Intercept Server (IS) until it receives an acknowledgment.

The GSX or SBC Core periodically sends keepalive messages to the IS whenever the call data channel is idle for the configurable keepalive timer time. The GSX restarts the keepalive timer after receiving a message from the IS. If the IS fails to respond, the GSX or SBC tries sending the message for a configured number of times, after which it fails over to the backup IS, if configured.

Call Data Message Types

The types of call data messages sent by the SBC Core and GSX devices and the events that trigger them are listed in the following table. Refer to Ribbon Lawful Intercept Interface Specification for further details.

Call Data Message Types

Used by GSX	Used by SBC Core	Event	Call Data Message (Sent to IS unless otherwise stated)
✓	✓	Reboot	Restart
✓	✓	Enable the device to send subsequent messages	Restart Response from Intercept Server
✓	✓	Keepalive	Keepalive
✓	✓	Policy response with LI	Signaling Start - contains calling party, called party, and digits dialed from policy response.
✓	✓	IP addresses and ports to send upstream and downstream call content via RTP	Signaling Start Response from Intercept Server
✓	✓	Policy response with LI	Media Report
✓		Call Teardown step 2	
✓		The leg becomes passive (channel closed)	
✓		Hook flash (upstream channel put on hold)	
✓		Hook flash (un-hold)	
✓		SDP Update	
✓	✓	Call Forward	Service Instance
		Conferencing (MS)	
✓	✓	Ringback	Signal Instance
		Alerting	

Used by GSX	Used by SBC Core	Event	Call Data Message (Sent to IS unless otherwise stated)
		Hook flash (new call or to put on hold)	
		Hook flash (un-hold)	
		Event Message to call leg (e.g., generate ring splash)	
✓	✓	Call Answer	Call Answer
✓	✓	Call Teardown step 1	
		The leg becomes passive (call previously answered)	
✓	✓	Call Teardown step 3	Signaling Stop
		Passive leg disconnect	
✓	✓	GSX intercept failures and alarms.	Indication
✓	✓	none	QOS Reserve (present but not used)
✓	✓	none	QOS Release (present but not used)
✓	✓	none	QOS Commit (present but not used)

Indication Messages

The GSX generates traps for any LI events that do not include data identifying an intercept subject (failure of call data channel, failure to get intercept resources, etc.). These traps also go into the signaling event log. When possible, the traps are also sent to the Intercept Server via the Indication message. Events containing sensitive information are sent to the Intercept Server but not put into the event log.

Indication messages for abnormal events include:

- Internal failure
- Memory Allocation failure
- Xmit Intercept Mgr msg failure
- Invalid state
- Intercept not enabled
- Could not map incoming msg to CC blk
- Invalid Channel address family
- Msg status code failure
- LSWU issue

- Codec map failure

Call Content Interface

The GSX and SBC Core each use a pair of RTP connections to send Call Content media streams to the Intercept Server for all intercepted calls using one RTP connection to the Intercept Server (IS) for each direction of the intercepted call.

The IS provides Call Content Channel IP address and UDP ports for the RTP connections in a Signaling Start Response message over the Call Data Channel.

The GSX/SBC network elements support the following audio encodings:

- G.711 a or u law
- G.729A
- G.729AB (silence suppression)
- G.723.1 with or without Annex A and both 5.3 and 6.4Kpbs
- G.726 @32Kbps
- ILBC
- ILBC (silence suppression)
- AMR
- EFR
- T38 Fax Relay
- G.722
- G.722 (silence suppression)
- G.722.1
- G.722.1 (silence suppression)
- G.722.2 (AMR-WB)
- G.728
- G.728 (silence suppression)
- EVRC
- EVRCB

The GSX and SBC network elements detect out-of-band tones and RFC2833 DTMF Relay RTP packets, and then sends the appropriate call data messages to the intercept server. However, the GSX/SBC does not perform in-band tone detection.

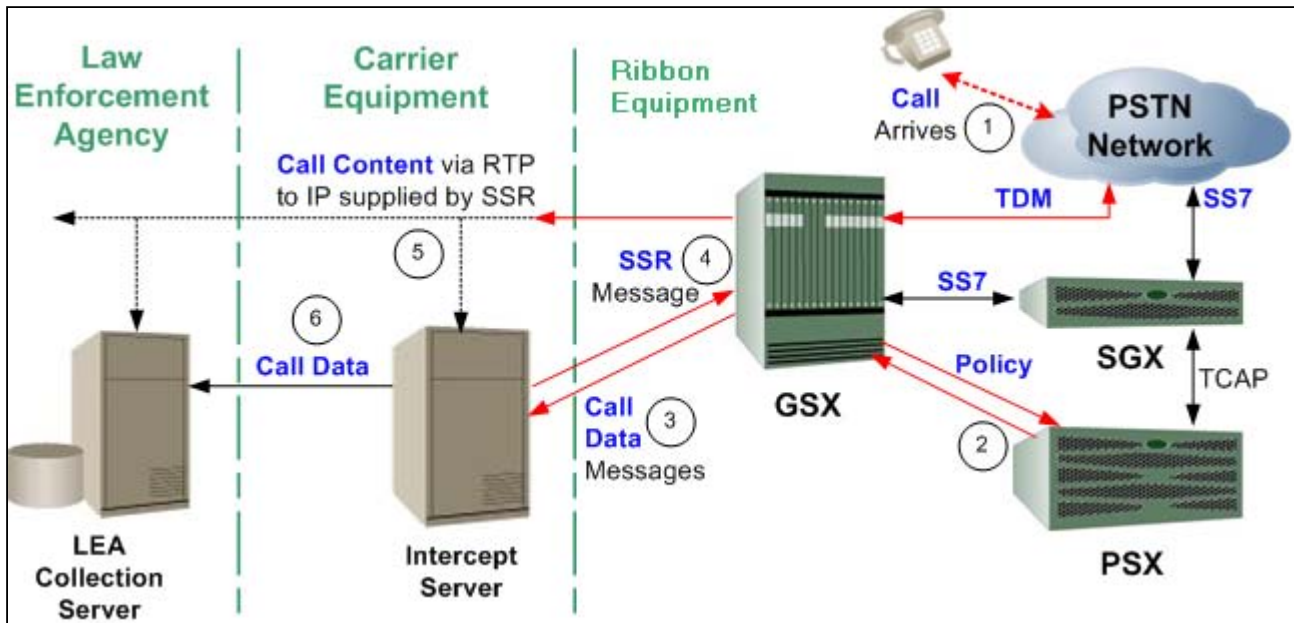
In “direct media” call scenarios, the GSX/SBC network elements are not part of the media path. In these scenarios, GSX/SBC network elements send a Media Report message with the IP address of another network element in the media path and with the “direct media” attribute set.

GSX Lawful Intercept Basic Call Processing

Currently, all LI calls are handled as Title III intercepts, which includes Calling party data (Pen Register), Called party data (Trap and Trace), and Call Content for all call parties.

Currently, the GSX identifies LI calls on the basis of Calling or Called number for calls originated, redirected and or terminated to a subject.

The following figure demonstrates the basic call processing sequence for calls handled by the GSX.



Before call processing begins, the GSX establishes redundant Call Data channels for messages and status over UDP/IP to the Intercept Server. For more information, refer to [Call Data Channel Establishment](#).

The call processing sequence is typically as follows:

1. Call information (such as an ISUP IAM or a SIP Invite) arrives at the GSX via network signaling.
2. The GSX sends a policy request to the PSX containing the received signaling information such as Calling and Called number. The PSX maintains the database of all subscribers, including any provisioned LI information from the IS/MD as relayed by the **Ribbon Application Management Platform (RAMP)**. When PSX processing of the Policy Request results in a match with any provisioned Lawful Intercept criteria, the PSX returns the matching Lawful Intercept criteria in the Policy Response.
3. The GSX sends the appropriate network signaling to route the call. The GSX also begins its duties as an intercept access point (IAP) by sending a **Signaling_Start** message over the Call Data Channel to the configured IS/MD address. Currently, all LI calls are handled as Title III intercepts, which includes Calling party data (Pen Register), Called party data (Trap and Trace), and Call Content for all call parties.

Ingress intercept call data signaling is started after the IS response has been processed, and the egress intercept call data signaling is started after routes are resolved.

4. The IS/MD sends a **Signaling_Start_Response** (SSR) message to the GSX (at the source address/port of the received **Signaling_Start** message) that includes the IP/ports to which to send the collected call content RTP streams. The GSX establishes two RTP connections for call content to the IP address and port specified in the SSR. The GSX then sends a **Media_Report** message to the IS indicating that the voice channels are open.
5. When signaling indicates that the call has been answered, the GSX sends a **Call_Answer** message to the IS. When signaling indicates the call is finished, the GSX sends a **Call_Disconnect** message to the IS, along with a **Media_Report** indicating that the voice channels are closed and no longer being streamed, and a **Signaling_Stop** message indicating that call signaling is complete and no further Call Data messages will be sent for this call.

6. The Intercept Server processes the Call Data as necessary, and forwards it to Law Enforcement Agency servers as required.

The GSX always performs a Title III intercept and sends calling party data, called party data, and call content (as directed) to the Intercept server. It is the responsibility of the IS to deliver only what the warrant requires (Title III, Pen Register, or Trap and Trace) to the Law Enforcement Agency.

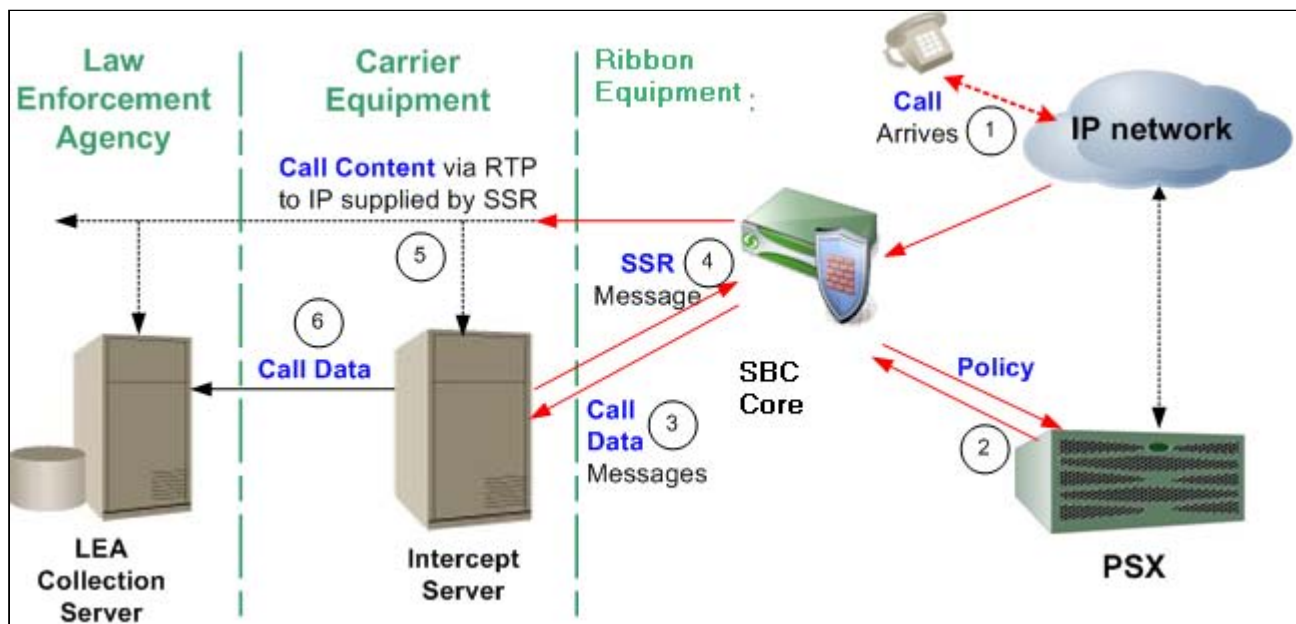
The GSX does not support LI for IP-looped “hairpin” calls on PNS10 or PNS30 servers.

SBC Lawful Intercept Basic Call Processing

The following figure demonstrates the basic call processing sequence for calls handled by the SBC.

All LI calls are handled as Title III intercepts, which include Calling party data (Pen Register), Called party data (Trap and Trace), and Call Content for all call parties.

LI calls are identified based on Calling or Called numbers for calls originated, redirected and or terminated to a subject.



Before call processing begins, the SBC establishes redundant Call Data channels for messages and status over UDP/IP to the Intercept Server. For more information, refer to [Call Data Channel Establishment](#).

The call processing sequence is typically as follows:

1. Call information (such as an ISUP IAM or a SIP Invite) arrives at the SBC via network signaling.
2. The SBC sends a policy request to the PSX containing the received signaling information such as Calling and Called number. The PSX maintains the database of all subscribers, including any provisioned LI information from the IS/MD as relayed by Ribbon Application Management Platform (RAMP). When PSX processing of the Policy Request results in a match with any provisioned Lawful Intercept criteria, the PSX returns the matching Lawful Intercept criteria in the Policy Response.

3. The SBC sends the appropriate network signaling to route the call.
The SBC also begins its duties as an intercept access point (IAP) by sending a **Signaling_Start** message over the Call Data Channel to the configured IS/MD address. Currently, all LI calls are handled as Title III intercepts, which include Calling party data (Pen Register), Called party data (Trap and Trace), and Call Content for all call parties.

Ingress intercept call data signaling is started after the IS response has been processed, and the egress intercept call data signaling is started after routes have been resolved.

4. The IS/MD sends a **Signaling_Start_Response** (SSR) message to the SBC (at the source address/port of the received **Signaling_Start** message) that includes the IP/ports to which to send the collected call content RTP streams.
The SBC establishes two RTP connections for call content to the IP address and port specified in the SSR. The SBC then sends a **Media_Report** message to the IS indicating that the voice channels are open.
5. When signaling indicates that the call has been answered, the SBC sends a **Call_Answer** message to the IS.
When signaling indicates the call is finished, the SBC sends a **Call_Disconnect** message to the IS, along with a **Media_Report** indicating that the voice channels are closed and no longer being streamed, and a **Signaling_Stop** message indicating that call signaling is complete and no further Call Data messages are sent for this call.
6. The Intercept Server processes the Call Data as necessary and forwards it to Law Enforcement Agency servers as required.

The SBC always performs a Title III intercept and sends calling party data, called party data, and call content (as directed) to the Intercept server. It is the responsibility of the IS to deliver only what the warrant requires (Title III, Pen Register, or Trap and Trace) to the Law Enforcement Agency.

Viewing CDC Status Report

Ribbon Application Management Platform (RAMP) automatically retrieves CDC configuration information for all registered SBC and GSX nodes.

You can view the Call Channel Data (CDC) for the nodes configured with LI in Ribbon Application Management Platform (RAMP).

To determine SBC CDC status, refer to [Show Status Address Context - Intercept](#).

1. Log on to the RAMP GUI as "calea" user.
2. Navigate to **Observability > Lawful Intercept > Report**.

CDC report for the GSX is displayed only if PIF collection is enabled for the GSX.

In addition to the CDC configuration (see [Table](#)), the report also displays the following information:

- Primary State
The state of the Primary Intercept Server (Enabled, Disabled, or N/A).
- Primary Mode
The operating mode of the Primary Intercept Server (Active, Out of Service, Standby, or N/A).
- Secondary State
The state of the Secondary Intercept Server.

- **Secondary Mode**
The operating mode of the Secondary Intercept Server.

Related topic:

- [View GSX CDC Report Using CLI](#)

View GSX CDC Report Using CLI

You can also use the following commands to determine GSX CDC status via the CLI:

```
SHOW INTERCEPT CALL DATA CHANNEL ALL ADMIN
```

```
SHOW INTERCEPT CALL DATA CHANNEL <text> ADMIN
```

These commands generate a report similar to the following:

```
Node: None Date: 2003/07/24 17:14:49 GMT
Zone: GMTMINUS05-EASTERN-US
Name:      liConfig
NIF Group Name      foo
UDP Port           3002
Primary Channel State      ENABLED
Primary Channel Mode      ACTIVE
Primary Channel IP Address 10.6.3.83
Secondary Channel State    DISABLED
Secondary Channel Mode     OUTOFSERVICE
Secondary Channel IP Address 10.6.3.84
Keep Alive Timer (seconds) 5
Number of Retries         3
```

LI Performance Management

In this section:

- [GSX LI Performance Reports](#)
 - [GSX CDC Performance Reports via CLI](#)
- [SBC LI Performance Reports](#)

Lawful Intercept related Call Data Channel message statistics available through Ribbon Application Management Platform (RAMP) Performance Manager. LI-related Call Data Channel message statistics, generated by the GSX and SBC for intercepted calls, are available to users with the proper Performance Management privileges on RAMP. The available LI-specific statistics are listed in the following table.

SBC	GSX	Message Count
✓	✓	Signaling Start sent (successful, unsuccessful)
✓	✓	Signaling Stop sent (successful, unsuccessful)
✓	✓	Call Answer sent (successful, unsuccessful)
✓	✓	Media Report sent (successful, unsuccessful)
✓	✓	Signaling Start Response received
✓	✓	Call Disconnect sent (successful, unsuccessful)
✓	✓	Service Instance sent (successful, unsuccessful)
✓	✓	Signal Instance sent (successful, unsuccessful)
		Conference Party Change sent (successful, unsuccessful)
✓	✓	Keep Alive sent (successful, unsuccessful)
✓	✓	Restart sent (successful, unsuccessful)
✓	✓	Indication sent (successful, unsuccessful)
✓	✓	Radius Acknowledgement received
✓	✓	Radius message code unknown received

A successful message counter is updated when a message is acknowledged by the IS.

GSX LI Performance Reports

Related article:

- [GSX CDC Performance Reports via CLI](#)

You can initiate the GSX LI performance reports shown in the following table through the Performance Report Wizard:

GSX Performance Reports

Report Name	Sub-Category	Description
Failed Intercept Message Stats Report	Lawful Intercept Stats Reports	Provides statistics concerning Lawful Intercept Failed Intercept Messages including: • # Signaling Start Msgs Failed • # Call Answer Msgs Failed • # Call Disconnect Msgs Failed • # Media Report Msgs Failed • # Service Instance Msgs Failed • # Signaling Instance Msgs Failed • # Indication Msgs Failed • # Signaling Stop Msgs Failed
Interface Maintenance Message Stats Report	Lawful Intercept Stats Reports	Provides statistics concerning Lawful Intercept Interface Maintenance Messages including: • # Primary Operation Status • # Secondary Operation Status • # Keep Alive Msgs Succeeded • # Keep Alive Msgs Failed • # Restart Msgs Succeeded • # Restart Msgs Failed • # Radius Acknowledge Received • # Radius Unknown Msg Received
Successful Intercept Message Stats Report	Lawful Intercept Stats Reports	Provides statistics concerning Lawful Intercept Successful Intercept Messages including: • # Signaling Start Msgs Succeeded • # Call Answer Msgs Succeeded • # Call Disconnect Msgs Succeeded • # Media Report Msgs Succeeded • # Service Instance Msgs Succeeded • # Signaling Instance Msgs Succeeded • # Indication Msgs Succeeded • # Signaling Start Response Received • # Signaling Stop Msgs Succeeded

The below tables provide information about how each GSX LI Performance Report field maps to a corresponding Statistics Table field. This information is provided to facilitate your ability to find definitions/descriptions of the various report fields.

Failed Intercept Messages Stats Report

Report Field	Statistics Table Field	Statistics Table
# Signaling Start Msgs Failed	SIGNAL_START_UNSUCCESS	GSX LI Performance Reports
# Call Answer Msgs Failed	CALL_ANSWER_UNSUCCESS	
# Call Disconnect Msgs Failed	CALL_DISCONNECT_UNSUCCESS	
# Media Report Msgs Failed	MEDIA_REPORT_UNSUCCESS	
# Service Instance Msgs Failed	SERVICE_INSTANCE_UNSUCCESS	
# Signaling Instance Msgs Failed	SIGNAL_INSTANCE_UNSUCCESS	
# Indication Msgs Failed	INDICATION_UNSUCCESS	
# Signaling Stop Msgs Failed	SIGNAL_STOP_UNSUCCESS	

Interface Maintenance Messages Stats Report

Report Field	Statistics Table Field	Statistics Table
# Primary Operation Status	PRI_OPER_STATE	GSX LI Performance Reports
# Secondary Operation Status	SEC_OPER_STATE	
# Keep Alive Msgs Succeeded	KEEP_ALIVE_SUCCESS	
# Keep Alive Msgs Failed	KEEP_ALIVE_UNSUCCESS	
# Restart Msgs Succeeded	RESTART_SUCCESS	
# Restart Msgs Failed	RESTART_UNSUCCESS	
# Radius Acknowledge Received	RADIUS_ACK_RECEIVED	
# Radius Unknown Msg Received	RADIUS_UNKNOWN_MSG_RECEIVED	

Successful Intercept Messages Stats Report

Report Field	Statistics Table Field	Statistics Table
# Signaling Start Msgs Succeeded	SIGNAL_START_SUCCESS	GSX LI Performance Reports
# Call Answer Msgs Succeeded	CALL_ANSWER_SUCCESS	
# Call Disconnect Msgs Succeeded	CALL_DISCONNECT_SUCCESS	
# Media Report Msgs Succeeded	MEDIA_REPORT_SUCCESS	
# Service Instance Msgs Succeeded	SERVICE_INSTANCE_SUCCESS	
# Signaling Instance Msgs Succeeded	SIGNAL_INSTANCE_SUCCESS	
# Indication Msgs Succeeded	INDICATION_SUCCESS	
# Signaling Start Response Received	SIGNAL_START_RESPONSE_RECEIVED	
# Signaling Stop Msgs Succeeded	SIGNAL_STOP_SUCCESS	

The table below provides information on the GSX LI statistic tables you can export, in the form of .csv (comma separated values) files, via the Data Collection Profile settings.

GSXImStatusStats

Column Name	Column Type	Index ?	Description
IMSTATUSINDEX	INTEGER	Yes	A unique value for each intercept manager entry between 1 and maximum allowed.
PRI_OPER_STATE	INTEGER	No	Current operational state of the Primary Call Data Channel.
SEC_OPER_STATE	INTEGER	No	Current operational state of the Secondary Call Data Channel.
SIGNAL_START_SUCCES S	COUNTER	No	The number of successful Signal Start messages sent on the active call data channel.
SIGNAL_START_UNSUCC ESS	COUNTER	No	The number of unsuccessful Signal Start messages sent on the active call data channel.
CALL_ANSWER_SUCCES S	COUNTER	No	The number of successful Call Answer messages sent on the active call data channel.
CALL_ANSWER_UNSUCC ESS	COUNTER	No	The number of unsuccessful Call Answer messages sent on the active call data channel.
CALL_DISCONNECT_SU CCESS	COUNTER	No	The number of successful Call Disconnect messages sent on the active call data channel.
CALL_DISCONNECT_UN SUCCESS	COUNTER	No	The number of unsuccessful Call Disconnect messages sent on the active call data channel.
MEDIA_REPORT_SUCCE SS	COUNTER	No	The number of successful Media Report messages sent on the active call data channel.
MEDIA_REPORT_UNSUCC CESS	COUNTER	No	The number of unsuccessful Media Report messages sent on the active call data channel.

Column Name	Column Type	Index ?	Description
SERVICE_INSTANCE_SUCCESS	COUNTER	No	The number of successful Service Instance messages sent on the active call data channel.
SERVICE_INSTANCE_UNSUCCESS	COUNTER	No	The number of unsuccessful Service Instance messages sent on the active call data channel.
SIGNAL_INSTANCE_SUCCESS	COUNTER	No	The number of successful Signal Instance messages sent on the active call data channel.
SIGNAL_INSTANCE_UNSUCCESS	COUNTER	No	The number of unsuccessful Signal Instance messages sent on the active call data channel.
INDICATION_SUCCESS	COUNTER	No	The number of successful Indication messages sent on the active call data channel.
INDICATION_UNSUCCESS	COUNTER	No	The number of unsuccessful Indication messages sent on the active call data channel.
KEEP_ALIVE_SUCCESS	COUNTER	No	The number of successful Keep Alive messages sent on the active call data channel.
KEEP_ALIVE_UNSUCCESS	COUNTER	No	The number of unsuccessful Keep Alive messages sent on the active call data channel.
RESTART_SUCCESS	COUNTER	No	The number of successful Restart messages sent on the active call data channel.
RESTART_UNSUCCESS	COUNTER	No	The number of unsuccessful Restart messages sent on the active call data channel.
RADIUS_ACK_RECEIVED	COUNTER	No	The number of Radius Acknowledgement messages received on the active call data channel.

Column Name	Column Type	Index ?	Description
RADIUS_UNKNOWN_MS G_RECEIVED	COUNTER	No	The number of messages received with an unknown Radius message code on the active call data channel.
SIGNAL_START_RESPON SE_RECEIVED	COUNTER	No	The number of Signaling Start Response messages received on the active call data channel.
SIGNAL_STOP_SUCCE S	COUNTER	No	The number of successful Signal Stop messages sent on the active call data channel.
SIGNAL_STOP_UNSUC CESS	COUNTER	No	The number of unsuccessful Signal Stop messages sent on the active call data channel.

GSX CDC Performance Reports via CLI

You can also get statistics on GSX call data channel performance by using these CLI commands:

```
SHOW INTERCEPT CALL DATA CHANNEL <> STATISTICS
SHOW INTERCEPT CALL DATA CHANNEL ALL STATISTICS
```

For example, this CLI command:

```
% SHOW INTERCEPT CALL DATA CHANNEL <CDC_id> STATISTICS
```

Will generate the following:

```
Node: COUGAR                               Date: 2007/08/21 15:42:22 GMT
                                           Zone: GMTMINUS05-EASTERN-US

      INTERCEPT CALL DATA CHANNEL STATISTICS
Call Data Channel Name:                   CDC_id
Primary Channel Operational State:        INSERVICE
Secondary Channel Operational State:      OUTOFSERVICE

              Sent                      Received
      Successful      Unsuccessful
-----
Signaling Start      2              0
Signaling Stop       2              0
Call Answer           2              0
Call Disconnect       2              0
Media Report          4              0
Service Instance      0              0
Signal Instance       0              0
```

Indication	0	0	
Keep Alive	14445	18	
Restart	1	0	
Radius Acknowledge			14458
Unknown Message			0
Signaling Start Response			2

SBC LI Performance Reports

The Ribbon Application Management Platform (RAMP) does not include SBC LI Performance Reports.

LI Fault Management

In this section:

- [GSX Lawful Intercept Alarms](#)
 - [sonusImPriOperStateChange](#)
 - [sonusImSecOperStateChange](#)
- [SBC Lawful Intercept Alarms](#)
- [RAMP Lawful Intercept Alarms](#)
 - [sonusEMSLIX1InterfaceDownNotification](#)
 - [sonusEMSLIX1InterfaceUpNotification](#)

Ribbon Application Management Platform (RAMP) manages any Lawful Intercept-related traps supported by the Ribbon devices through the generic Fault Management component in RAMP. There is no indication of the intercept criteria in any of these traps, so there are no added security requirements for viewing LI-related traps. LI-related alarms for intercepted calls are available to users with the proper Fault Management privileges via RAMP.

GSX Lawful Intercept Alarms

In this section:

- [sonusImPriOperStateChange](#)
- [sonusImSecOperStateChange](#)

The GSX Lawful Intercept alarms are covered in this section.

sonusImPriOperStateChange

Description	This trap indicates the intercept manager's primary call data channel operational state has changed. The varbind sonusImStatusPriOperState indicates the new state.
Instance Fields	sonusImAdmnName
Severity	Minor
Event Codes	sonusImAdmnName—The name of this Intercept Manager instance. sonusImStatusPriOperState—Current operational state of the Primary call data channel: • inService(1) • outOfService(2) • standBy(3)
Repetition	No
Impact	The GSX cannot send intercepted call contents and call data over to Intercept Manager server if the operational state of both primary and secondary call data channel are OOS.
Action	If IM operational state changed to outOfService(2), check both the Intercept Manager Server and the IM configuration in the GSX to get more information. The following CLI commands can be used to get IM configuration and statistics. <pre>SHOW INTERCEPT CALL DATA CHANNEL ALL ADMIN SHOW INTERCEPT CALL DATA CHANNEL ALL STATISTICS</pre>
Clearing	Automatic

sonusImSecOperStateChange

Description	This trap indicates the Intercept Manager's secondary call data channel operational state has changed. The varbind sonusImStatusSecOperState indicates the new state.
Instance Fields	sonusImAdmnName
Severity	Minor

Event Codes	sonusImAdmnName—The name of this Intercept Manager instance. sonusImStatusSecOperState—Current operational state of the Secondary call data channel: • inService(1) • outOfService(2) • standBy(3)
Repetition	No.
Impact	The GSX cannot send intercepted call contents and call data over to Intercept Manager server if the operational state of both primary and secondary call data channel are OOS.
Action	If IM operational state changed to outOfService(2), check both the Intercept Manager Server and the IM configuration in the GSX to get more information. The following CLI commands can be used to get IM configuration and statistics. <pre>SHOW INTERCEPT CALL DATA CHANNEL ALL ADMIN SHOW INTERCEPT CALL DATA CHANNEL ALL STATISTICS</pre>
Clearing	Automatic

SBC Lawful Intercept Alarms

The following Lawful Intercept alarms exist on the SBC Core:

- [sonusSbxImMediationServerTcpLinkDown](#) - MAJOR
- [sonusSbxImMediationServerTcpLinkUp](#) - MAJOR
- [sonusSbxImPriOperStateChange](#) - MAJOR
- [sonusSbxImSecOperStateChange](#) - MAJOR
- [sonusSbxImMediationServerX2MsgBufferFull](#) - MAJOR
- [sonusSbxImMediationServerX2MsgBufferAvailable](#) - MAJOR
- [sonusLiCryptoFailureNotification](#) - MAJOR
- [sonusLiCryptoSuccessNotification](#) - MAJOR

RAMP Lawful Intercept Alarms

Additional Topics:

- [sonusEMSLIX1InterfaceDownNotification](#)
- [sonusEMSLIX1InterfaceUpNotification](#)

Ribbon Application Management Platform (RAMP) Lawful Intercept alarms are covered in this section.

sonusEMSLIX1InterfaceDownNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.107
Definition:	This notification is raised when the X1 interface connection terminates.
Action:	None required.
Clearing:	Automatic, sonusEMSLIX1InterfaceUpNotification
Repetition:	No
Instance Fields:	mediationServerIP
Event Code(s):	• sysName: An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. • sysObjectID: The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.' • sonusEventTime: Provides timestamp of when the event occurs. • sonusEventDescription: Describes the event. • sonusEventClass: Lists the associated event class. • mediationServerIP: IP address of the mediation server.

sonusEMSLIX1InterfaceUpNotification

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.108
Definition:	This notification is raised when the X1 interface connection establishes.
Action:	None required.
Clearing:	Automatic
Repetition:	No
Instance Fields:	mediationServerIP

Event Code(s):	sysName: An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID: The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.' sonusEventTime: Provides timestamp of when the event occurs. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. mediationServerIP: IP address of the mediation server.

LI Security

In this section:

- [Separate LI Provisioning and System Management](#)
- [Provisioning Only via API from Intercept Server](#)
- [Write-Only RAMP LI Provisioning](#)
- [PSX Security](#)
- [IS Handling of Ribbon IP Addresses](#)
- [GSX and SBC Handling of Call Content IP Address](#)
- [Billing](#)
- [Protocol Security](#)

The Ribbon Lawful Intercept solution provides several features to maintain security of Lawful Intercept activities.

Separate LI Provisioning and System Management

Though management of the Ribbon equipment and provisioning of LI targets are both handled by Ribbon Application Management Platform (RAMP), they are controlled through two separate and distinct interfaces: Surveillance administration is via LI API messages from the IS to RAMP. Ribbon system administration is via RAMP GUI management system from a separate System Administration interface. Data provided through the LI API is invisible to the RAMP GUI.

Provisioning Only via API from Intercept Server

LI targets can only be provisioned via LI API messages sent to the specified IP/port on RAMP. LI targets cannot be provisioned via any other means, such as the GSX CLI or direct PSX database writes.

Write-Only RAMP LI Provisioning

LI target provisioning data are not stored in RAMP but are sent directly to the PSX database. Target data cannot be read from the PSX database via RAMP, and are obscured from PSX database queries. The IS can send RAMP a message via the LI API to retrieve, update, or delete a specific currently provisioned Lawful Intercept target, or list all currently provisioned Lawful Intercept targets. Based upon the query, information is retrieved from the PSX database and returned in an API response to the IS.

The SBC, and GSX do not store information about intercept subjects.

PSX Security

There is no GUI screen to view/modify/delete the contents of Lawful Intercept Criteria table. There is also no logging of LI-related events in log files such as pes.log, pipe.log, and so on.

IS Handling of Ribbon IP Addresses

During LI call processing, the IS responds to Call Data messages from SBCs and GSXs using the Source IP addresses of the messages. The IS never initiates Call Data exchange with the SBC or GSX, so it need not be provisioned with their IP addresses beforehand.

GSX and SBC Handling of Call Content IP Address

The GSX and SBC devices are configured with the IP address (for example, of the IS) to which to send Call Data messages. However, during call processing, only in response to the GSX call data, the IS sends the GSX an SSR message containing the IP address to which the GSX should send its Call Content RTP streams.

Billing

Lawful Intercept calls generate the same call detail records as non-LI calls.

Protocol Security

You can run secure protocols for all communication links between the intercept server and RAMP and between RAMP and the Ribbon devices.

- Intercept Server to RAMP
The SOAP interface is secured using SSL. The authentication and authorization mechanism is on RAMP user and role management.
- RAMP to PSX
The PIPE connection between RAMP and PSX can be secured over SSH.
- RAMP to SBC
The only information configured within the SBC by the RAMP is the IP and Port of the IS(s), which is not considered to be a security risk if sent over the network.

Deploying liTestWebApp in RAMP

To deploy liTestwebapp in Ribbon Application Management Platform (RAMP):

1. Enable Lawful Intercept (LI) on RAMP. Refer to [Enabling Lawful Intercept on RAMP](#).
2. Download "testTools-<RAMP VERSION>.tar.gz" from the Ribbon support portal and copy it to a temporary directory in RAMP.
3. Unzip the file as shown in the following example:


```
gzip -d testTools-V21.11.00R000.tar.gz
```

4. Untar the file as shown in the following example.

```
tar -xvf testTools-V21.11.00R000.tar
```

5. Change to insight user.
6. Copy *liTestwebapp.war* to */opt/sonus/ems/weblogic/insight/deployments*.
7. Navigate to the directory */opt/sonus/ems/weblogic/insight/deployments*.
8. Execute the following:

```
chown -R insight:insight liTestWebApp.war
```

9. Enter the following command:

```
chmod -R 775 liTestWebApp.war
```

10. Enter the following command:

```
touch liTestWebApp.war.dodeploy
```

11. To launch liTestwebapp in browser, enter <https://<host-ip>/liTestWebApp/>.

Related Documentation

For additional information about Lawful Intercept, refer to the following related documentation:

- [PSX Documentation](#)
- [GSX9000 Series Documentation](#)
- [SBC Core Documentation](#)

Refer to the Intercept Server manufacturer documentation for information about provisioning LI targets, and for details on the Intercept Server's implementation of the Ribbon LI API and Call Data interface.

Alarms and Troubleshooting

In this section:

- [RAMP Alarms Guide](#)
 - [New and Deprecated Alarms](#)
 - [Managing Device Faults](#)
 - [RAMP Alarms](#)
 - [Cross-Platform Alarms](#)
- [Fault Management](#)
 - [Fault Management Workflows](#)
 - [Work with Active Alarms](#)
 - [Work with Alarm History](#)
 - [Purge Alarms](#)
 - [Reclassify Alarm Content](#)
 - [Send Email Notifications for Alarms](#)
 - [Forward Alarms to an External Destination](#)
 - [Monitor Fault Management Activity](#)
- [Troubleshooting Guide](#)
 - [EdgeMarc Troubleshooting](#)
 - [Database Troubleshooting](#)
 - [Fault Manager Troubleshooting](#)
 - [General Troubleshooting](#)
 - [GSX Troubleshooting](#)
 - [RAMP CNF Troubleshooting](#)
 - [RAMP GR Auto-Switchover Troubleshooting](#)
 - [Retrieve System Information](#)
 - [Tools Troubleshooting](#)
 - [Unlock or Recover a User Account for Sysadmin or Any Admin User](#)

RAMP Alarms Guide

Contents

- [New and Deprecated Alarms](#)
- [Managing Device Faults](#)
 - [Fault Instrumentation](#)
 - [Fault Notification](#)
- [RAMP Alarms](#)
 - [Access Management Alarms](#)
 - [Cluster Alarms](#)
 - [Cron Job Alarms](#)
 - [Database Alarms](#)
 - [Device Management Alarms](#)
 - [EdgeMarc Alarms](#)
 - [GSX Discovery](#)

- [High Availability Alarms](#)
- [Licensing Management Alarms](#)
- [Normalized Alarms](#)
- [Number Portability Alarms](#)
- [OSS Trap Resync Alarms](#)
- [Performance Management Alarms](#)
- [RAMP CNF - Alarms](#)
- [Reachability Alarms](#)
- [Redundancy Alarms](#)
- [SBC Edge Alarms](#)
- [Threshold Alarms](#)
- [Verification Manager Alarms](#)
- [linkUp](#)
- [linkDown](#)
- [Cross-Platform Alarms](#)
 - [Agent Framework Alarms](#)
 - [Host Monitoring Alarms](#)
 - [Resource Usage Threshold Matrix](#)

This guide provides detailed alarm information for devices you manage with **Ribbon Application Management Platform (RAMP)** to aid in isolating and troubleshooting system fault conditions. Each alarm description provides the alarm definition, severity level, associated event codes, impact to the system, action(s) to rectify the fault condition, alarm repetition, and clearing information.

Other Ribbon troubleshooting references include:

- C3 G9 - [G9 Converged Gateway 26.0 Documentation](#)
- C20 - [C20 R22 Fault Reference](#)
- Cross-platform alarms across devices – [Cross-Platform Alarms](#)
- DELL - [Dell Server Deployment Guide](#)
- DSC - [DSC Alarms Guide](#)
- DSI - [DSI Alarms Guide](#)
- G6MM - [G6 Universal Gateway 14.3 Documentation](#)
- GSX - [GSX9000 Alarm and Event Troubleshooting](#)
- PSX Policy Server – [PSX Alarms Guide / Troubleshooting the PSX](#)
- SBC Core - [SBC Core Alarms Guide](#)
- SGX - [SGX4000 Alarms Guide](#)

New and Deprecated Alarms

In this section:

- [New Alarms](#)
 - [New Alarms in 24.09R000 Release](#)
- [Deprecated Alarms](#)
 - [Deprecated Alarms in 24.09R000 Release](#)

New Alarms

New Alarms in 24.09R000 Release

There are no new alarms in this release.

Deprecated Alarms

Deprecated Alarms in 24.09R000 Release

The following are the deprecated alarms in this release:

- sonusV2VfyMgrApplVersionFailNotification
- sonusV2VfyMgrApplVersionSuccessNotification
- sonusV2VfyMgrMgmtClientFailNotification
- sonusV2VfyMgrMgmtClientSuccessNotification
- sonusV2VfyMgrSnmpAccessFailNotification
- sonusV2VfyMgrSnmpAccessSuccessNotification
- sonusV2VfyMgrAgentVersionFailNotification
- sonusV2VfyMgrAgentVersionSuccessNotification
- sonusVfyMgrSnmpAccessFailNotification

Managing Device Faults

In this section:

- [Fault Instrumentation](#)
- [Fault Notification](#)

Fault Instrumentation

In this section:

- [What is Monitored](#)
- [Running Customer Supplied Instrumentation Agents](#)

What is Monitored

Depending on hardware/software and which instrumentation components are running on a device, the following categories of fault information are available:

- Environmental alarms (temperature, fan)
- Host resource utilization (CPU, memory, file system)
- Java Agent Framework (Chassis, Process Mgmt)

- Database Replication
- Process monitoring
- Geographical Redundancy (GR) faults
- Device-specific faults (Refer to the appropriate alarm references for device-specific faults.)

Running Customer Supplied Instrumentation Agents

Ribbon strongly recommends not using customer-supplied instrumentation agents on Ribbon hosts to avoid performance/interoperability repercussions. If necessary, please contact Ribbon Global Product Support for additional details.

Fault Notification

SNMP Traps

The Ribbon Application Management Platform (RAMP) devices use SNMP traps to notify management applications of faults. Use RAMP or a third-party management application to view traps from all devices. If any node or application malfunctions, a fault notification is initiated at the device and forwarded to the RAMP or third-party management application for processing.

The following SNMP trap types are supported:

- All Ribbon devices support SNMP v2 or v3 traps.
- RAMP supports V1, V2, and V3 trap forwarding.

RAMP Alarms

This page describes the alarm notifications generated by Ribbon Application Management Platform (RAMP) and provides links to each alarm category.

RAMP Alarm Categories

The RAMP alarms are categorized according to the device or application that generated the alarm:

- [Access Management Alarms](#)
- [Cluster Alarms](#)
- [Cron Job Alarms](#)
- [Database Alarms](#)
- [Device Management Alarms](#)
- [EdgeMarc Alarms](#)
- [GSX Discovery](#)
- [High Availability Alarms](#)
- [Licensing Management Alarms](#)
- [Normalized Alarms](#)
- [Number Portability Alarms](#)
- [OSS Trap Resync Alarms](#)
- [Performance Management Alarms](#)
- [RAMP CNF - Alarms](#)
- [Reachability Alarms](#)
- [Redundancy Alarms](#)
- [SBC Edge Alarms](#)
- [Threshold Alarms](#)
- [Verification Manager Alarms](#)
- [linkUp](#)

- [linkDown](#)

Alarm Field Definitions

RAMP alarm notifications are defined by the fields:

- **Type**—Represents the severity level assigned by the device. Possible severity levels are Critical, Major, Minor, and Informational.
- **Description**—Describes the purpose of the alarm.
- **Impact**—Describes the impact of the alarm on the system when the indicated failure or fault occurs.
- **Action**—Details the action the operator must take to eliminate/prevent the failure condition. When appropriate, step-by-step procedures will be provided.
- **Clearing**—This field identifies how an alarm clears from the Fault Manager Event List. Alarm clearing is either automatic or manual.
- **Repetition**—Identifies if an alarm is repeated for each occurrence of a particular failure relating to the same managed object instance. When appropriate, repetition interval information is included in this field.
- **Instance Fields**—By default, all alarms are instanced by the source host and trap type. For some alarms, an Instance ID field is included to uniquely identify the alarms. The Instance ID is created by appending the values of the instance fields to the default instance information. In this guide, when instance fields exist for an alarm, the Instance Fields category in the alarm description is populated with one or more instance fields.
- **Event Code(s)**—Identifies detailed event information contained in the alarm (event levels and classes, threshold types, clearing strings, and so forth). This field may not always be included.

The following alarms are raised on RAMP, but the error condition is on the device. and not on the RAMP:

- [sonusEmsV2RisingEventNotification](#)
- [sonusEmsV2FallingEventNotification](#)
- [sonusEmsV2NodeUnreachableNotification](#)
- [sonusEmsV2HostUnreachableNotification](#)
- [sonusEmsV2NodeReachableNotification](#)
- [sonusEmsV2HostReachableNotification](#)
- [sonusEmsV2NodeRestartedNotification](#)
- [sonusEmsV2NodeCfgFailNotification](#)
- [sonusV2VfyMgrNodeTypeFailNotification](#)
- [sonusV2VfyMgrNodeTypeSuccessNotification](#)
- [sonusEmsV2PifCollectFailNotification](#)
- [sonusEmsPMPProfileAssignmentFailedNotification](#)
- [sonusEmsV2PifCollectDoneNotification](#)
- [sonusEmsV2PMStatsFileCollectionFailed](#)

Access Management Alarms

Contents

- [sonusEmsV2LoginFailureNotification](#)
- [sonusEmsLDAPServerErrorNotification](#)
- [ribbonCertificateExpiryStatusNotification](#)
- [ribbonCertificateExpiredNotification](#)
- [ribbonRadiusAuthServerUnreachable](#)
- [ribbonRadiusAuthServerReachable](#)

This section covers alarms related to accessing Ribbon Application Management Platform (RAMP).

sonusEmsV2LoginFailureNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.81
Definition	A login attempt failed for the user specified in the field sonusEmsLoginUserName from the host specified in the field sonusEmsV2LoginIPAddress.
Repetition	Yes. Repeats every time a login failure occurs.
Event Codes	sonusEmsLoginUserName: The user name provided during a login attempt. sonusEmsV2LoginIPAddress: The IP address of the node from which the login attempt is initiated. sonusEmsV2LoginIPAddressType: The address type of sonusEmsV2LoginIPAddress. • 1 indicates IPv4. • 2 indicates IPv6.
Instance Fields	sonusEmsLoginUserName, sonusEmsV2LoginIPAddress, sonusEmsV2LoginIPAddressType
Action	If the alarm occurs repeatedly, investigate user/host activities for which the login the failure occurred.
Impact	No impact to the system.
Clearing	Manual.

sonusEmsLDAPServerErrorNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.131
Description	An error occurred while authenticating the user on the LDAP server.
Repetition	Yes. Repeats every time Ribbon Application Management Platform tries to verify the authentication mechanism.
Event Codes	N/A
Instance Fields	N/A
Action	Check the Security Realm configuration and LDAP server status.
Impact	The LDAP-based user Authentication fails.
Clearing	Manual

ribbonCertificateExpiryStatusNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.161
Definition	Ribbon Application Management Platform (RAMP) sends a daily notification when certificates are about to expire within the configured threshold. To set how many days in advance you want to be notified of the certificate expiry, navigate to Management > Authentication & Authorization > Administration and enter the number of days in the field "Number of days for certificate expiry notification." Range: 15 to 365 days, default: 15 days
Repetition	Yes, repeats daily (once every 24 hours) based on the configured threshold.
Event Codes	- sonusEventTime: The timestamp of the event. - sonusEventDescription: The description of the event. - sonusEventClass: The event class. - sonusEventLevel: The event level.
Instance Fields	sonusHostID: The unique ID or serial number for this host.
Action	Update the certificates.
Impact	Certificates will expire.

Clearing	Manual

ribbonCertificateExpiredNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.160
Definition	Ribbon Application Management Platform (RAMP) sends a daily notification when the certificates in the truststore have expired.
Repetition	Yes, repeats daily (once every 24 hours).
Event Codes	- sonusEventTime: The timestamp of the event. - sonusEventDescription: The description of the event. - sonusEventClass: The event class. - sonusEventLevel: The event level.
Instance Fields	sonusHostID: The unique ID or serial number for this host.
Action	Update the certificate
Impact	The certificate cannot be used.
Clearing	Manual

ribbonRadiusAuthServerUnreachable

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.173
Definition	This trap is raised when there is a connection failure.
Repetition	Yes. Repeats every time if there is a connection failure.
Event Codes	sonusHostID

Instance Fields	sonusHostID, sonusEventDescription, sonusEventClass, sonusEventLevel, sonusEventTime, ribbonRadiusIpAddressOrFQDN
Action	None
Impact	None
Clearing	Automatic, ribbonRadiusAuthServerReachable

ribbonRadiusAuthServerReachable

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.174
Definition	It is the clearing alarm for ribbonRadiusAuthServerUnreachable.
Repetition	Yes. Repeats on successful connection.
Event Codes	sonusHostID
Instance Fields	sonusHostID, sonusEventDescription, sonusEventClass, sonusEventLevel, sonusEventTime, ribbonRadiusIpAddressOrFQDN
Action	None
Impact	None
Clearing	Automatic

Cluster Alarms

Contents

- [sonusEmsClusterInstanceUpNotReceivedNotification](#)
- [sonusEmsClusterNodeDeRegistrationNotification](#)
- [sonusEmsClusterNodeDiscoveryFailedNotification](#)
- [sonusEmsClusterNodeIPsInUseNotification](#)
- [sonusEmsClusterNodeIPsInUseUnRegisterNotification](#)
- [sonusEmsClusterNodePurgeNotification](#)
- [sonusEmsClusterNodeRegistrationRejectedNotification](#)
- [sonusEmsNodeSnmpV3SetFailedNotification](#)

This section covers alarms related to cluster management.

sonusEmsClusterInstanceUpNotReceivedNotification

Type: **CRITICAL**

OID	1.3.6.1.4.1.2879.2.1.7.2.0.96
Description	This notification indicates the Ribbon Application Management Platform (RAMP) does not receive instance up request for dynamic register nodes within node registration completion interval.
Repetition	Yes. Repeats every time node discovery fails and node is deregistered from RAMP.
Event Codes	ClusterName: This describes the name of the cluster which is associated with the node.
Instance Fields	sonusEmsClusterInstanceUpNotReceivedNotification
Action	View the log file for relevant error information indicating a problem. The log file is specified in the <code>log4j.xml</code> file in the appropriate configuration directory: 1. <code>/opt/sonus/ems/weblogic/sonusEms/logs/sys/ems_trace_log</code> 2. Take corrective action to fix the problem.
Impact	RAMP deregisters the existing cloud node.
Clearing	Manual

sonusEmsClusterNodeDeRegistrationNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.99
Description	A deregistration is requested by the cloud node to Ribbon Application Management Platform (RAMP).
Repetition	Yes. Repeats every time a cloud node initiates a deregistration request.
Event Codes	ClusterName: This describes the name of the cluster which is associated with the node.
Instance Fields	sonusEMSClusterNodeDeRegistrationNotification
Action	View the log file for relevant error information indicating a problem. The log file is specified in the <code>log4j.xml</code> file in the appropriate configuration directory: <code>/opt/sonus/ems/weblogic/sonusEms/logs/sys/ems_trace_log</code> - Take corrective action to fix the problem.
Impact	RAMP deregisters the cloud node.
Clearing	Manual

sonusEmsClusterNodeDiscoveryFailedNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.101
Description	The cloud node discovery fails, and the specified node state changes to offline.
Repetition	Yes. Repeats when cloud nodes discover operation fail.
Event Codes	ClusterName: This describes the name of the cluster which is associated with the node.
Instance Fields	sonusEMSClusterNodeDiscoveryFailedNotification

Action	View the log file for relevant error information indicating a problem. The log file is specified in the <code>log4j.xml</code> file in the appropriate configuration directory: 1. <code>/opt/sonus/ems/weblogic/sonusEms/logs/sys/ems_trace_log</code> 2. Take corrective action to fix the problem.
Impact	the cloud node state changes to offline, and the node is not reachable by Ribbon Application Management Platform (RAMP).
Clearing	Manual

sonusEmsClusterNodeIPsInUseNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.97
Description	Ribbon Application Management Platform (RAMP) rejects dynamic node registration because the device IP is already in use.
Repetition	Yes. Repeats each time node registration fails.
Event Codes	ClusterName: This describes the name of the cluster which is associated with the node.
Instance Fields	sonusEmsClusterInstanceUpNotReceivedNotification
Action	View the log file for relevant error information indicating a problem. The log file is specified in the <code>log4j.xml</code> file in the appropriate configuration directory: 1. <code>/opt/sonus/ems/weblogic/sonusEms/logs/sys/ems_trace_log</code> 2. Take corrective action to fix the problem.
Impact	The RAMP fails to register the cloud node.
Clearing	Manual

sonusEmsClusterNodeIPsInUseUnRegisterNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.102

Description	Ribbon Application Management Platform (RAMP) rejects dynamic node re-registration with because the device IP is already in use.
Repetition	Yes. Repeats each time node re-registration fails.
Event Codes	ClusterName: This describes the name of the cluster which is associated with the node.
Instance Fields	sonusEmsClusterNodeIPsInUseUnRegisterNotification
Action	View the log file for relevant error information indicating a problem. The log file is specified in the <code>log4j.xml</code> file in the appropriate configuration directory: <code>/opt/sonus/ems/weblogic/sonusEms/logs/sys/ems_trace_log</code> - Take corrective action to fix the problem.
Impact	RAMP fails re-register a cloud node.
Clearing	Manual

sonusEmsClusterNodePurgeNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.100
Description	The Ribbon Application Management Platform (RAMP) invokes a purge operation on the specified cloud nodes which exceed unregistered node interval.
Repetition	Yes. Repeats each time when nodes exceeds unregistered node interval.
Event Codes	ClusterName: This describes the name of the cluster which is associated with the node.
Instance Fields	sonusEMSClusterNodePurgeNotification

Action	View the log file for relevant error information indicating a problem. The log file is specified in the <code>log4j.xml</code> file in the appropriate configuration directory: 1. <code>/opt/sonus/ems/weblogic/sonusEms/logs/sys/ems_trace_log</code> 2. Take corrective action to fix the problem.
Impact	Cloud nodes are purged from RAMP.
Clearing	Manual

sonusEmsClusterNodeRegistrationRejectedNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.95
Description	Ribbon Application Management Platform (RAMP) rejected a dynamic node registration request.
Repetition	Yes. Repeats each time the node registration fails.
Event Codes	ClusterName: This describes the name of the cluster which is associated with the node.
Instance Fields	sonusEmsClusterNodeRegistrationRejectedNotification
Action	View the log file for relevant error information indicating a problem. The log file is specified in the <code>log4j.xml</code> file in the appropriate configuration directory: 1. <code>/opt/sonus/ems/weblogic/sonusEms/logs/sys/ems_trace_log</code> 2. Take corrective action to fix the problem.
Impact	RAMP failed to register the specified cloud node.
Clearing	Manual

sonusEmsNodeSnmpV3SetFailedNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.124

Description	Unable to set SNMPv3 security level parameters on the node while creating or editing cluster configurations on Ribbon Application Management Platform (RAMP), as communication with the managed device fails (node is down).
Repetition	Yes. Repeats each time communication with the device fails.
Event Codes	ClusterName: Describes the name of the cluster associated with the node.
Instance Fields	sonusEmsNodeSnmpV3SetFailedNotification
Action	Resync the SNMP settings of the cluster profile again.
Impact	RAMP fails to support authentication and encryption of SNMPv3 traps from the managed devices.
Clearing	Manual

Cron Job Alarms

In this section:

- [ribbonCronJobExecutionMissed](#)

ribbonCronJobExecutionMissed

Type: MINOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.175
Description	This event is generated when a scheduled cron job fails to execute at a specific time. A variety of reasons can cause this failure, such as resource constraints or software errors. Monitoring and addressing these events can help ensure the system performs as expected.
Repetition	Yes

Event Codes	- sonusHostID - sonusEventDescription - sonusEventClass - sonusEventLevel - sonusEventTime - ribbonMissedCronJobName
Instance Fields	None
Action	View the cron logs at: <code>/var/log/cron</code> to identify the cause of failure. The job name and the misfire time(s) are reported by varbind "<code>ribbonMissedCronJobName</code>" and "<code>sonusEventDescription</code>"
Impact	Misfired cron job can lead to improper functioning of the system.
Clearing	Manual

Database Alarms

Contents

- sonusEmsInsightDBConnectionPoolExhaustedNotification
- sonusDBaasDownNotification
- sonusDBaasClearNotification
- sonusDBaasFileSystemUtilizationNotification
- sonusDBaasFileSystemUtilizationClearNotification
- sonusDBaasDatabaseConnectionNotification
- sonusDBaasDatabaseConnectionClearNotification
- sonusDBaasCertificateNotification
- sonusDBaasCertificateClearNotification
- sonusDBaasReplicationLagNotification
- sonusDBaasReplicationLagClearNotification
- sonusDBaasDownstreamNodesConnectedNotification
- sonusDBaasDownstreamNodesConnectedClearNotification
- sonusDBaasInactiveReplicationSlotsNotification
- sonusDBaasInactiveReplicationSlotsClearNotification

sonusEmsInsightDBConnectionPoolExhaustedNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.119
Description	The alarm is raised when there are not sufficient database connections in the RAMP connection pool.
Repetition	None
Event Codes	sysName: An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID: The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it can assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.' sonusEventTime: The timestamp of the event. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level.
Instance Fields	None
Action	Increase the connection pool size.

Impact	Loss of functionality in Ribbon Application Management Platform (RAMP), the RAMP GUI may not be able to function. PM collection may not be successful.
Clearing	Manual

sonusDBaaSDownNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.126
Description	The DbaaS services are down on Ribbon Application Management Platform (RAMP).
Repetition	No
Event Codes	sonusHostID —The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Instance Fields	sonusHostID, sonusEventDescription, sonusEventClass, sonusEventLevel, sonusEventTime
Action	1. As the postgres user on RAMP, check database status with the command “dbaas_service status”. 2. Perform one of the following: ◦ If the database is down, attempt to start it. Refer to Start DBaaS Service in RAMP. ◦ If the database does not start, check the logs in /var/log/postgres.
Impact	Database is down. • If this is the active node, then all RAMP services are also down. • If this is a standby node, then it is not a viable fail-over option.
Clearing	Automatic; sonusDBaaSClearNotification

sonusDBaaSClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.129

Description	Clear alarm for sonusDBaaSDownNotification
Repetition	No
Event Codes	sonusHostID —The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Instance Fields	sonusHostID, sonusEventDescription, sonusEventClass, sonusEventLevel, sonusEventTime
Action	None
Impact	None
Clearing	Automatic

sonusDBaaSFileSystemUtilizationNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.125
Description	The disk utilization is more than configured value.
Repetition	No
Event Codes	sonusHostID —The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Instance Fields	sonusHostID, sonusEventDescription, sonusEventClass, sonusEventLevel, sonusEventTime
Action	Find excessive disk utilization by executing the following command as the root user: du -sh *
Impact	No immediate impact, but could cause RAMP services to go down if disk utilization increases to 100%.

Clearing	Automatic, sonusDBaaSFileSystemUtilizationClearNotification

sonusDBaaSFileSystemUtilizationClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.132
Description	Clear alarm for sonusDBaaSFileSystemUtilizationNotification
Repetition	No
Event Codes	sonusHostID —The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Instance Fields	sonusHostID, sonusEventDescription, sonusEventClass, sonusEventLevel, sonusEventTime
Action	None
Impact	None
Clearing	Automatic

sonusDBaaSDatabaseConnectionNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.133
Description	The applications are unable to connect to the database.
Repetition	No
Event Codes	sonusHostID —The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Instance Fields	sonusHostID, sonusEventDescription, sonusEventClass, sonusEventLevel, sonusEventTime

Action	1. Check RAMP Status 2. Check the dbaas connectivity status in the output.
Impact	The database or pgbouncer is down.
Clearing	Automatic, sonusDBaaSDatabaseConnectionClearNotification

sonusDBaaSDatabaseConnectionClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.134
Description	Clear alarm for sonusDBaaSDatabaseConnectionNotification
Repetition	No
Event Codes	sonusHostID —The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Instance Fields	sonusHostID, sonusEventDescription, sonusEventClass, sonusEventLevel, sonusEventTime
Action	None
Impact	None
Clearing	Automatic

sonusDBaaSCertificateNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.135
Description	The DbaaS service certificate is not valid.
Repetition	No
Event Codes	sonusHostID —The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.

Instance Fields	sonusHostID, sonusEventDescription, sonusEventClass, sonusEventLevel, sonusEventTime
Action	1. Issue the root certificate again. 2. Replace the old certificate with the new certificate.
Impact	• The database is down. • If the error condition is on the active node, all the RAMP services are down. • If the error condition is on the standby node, failover is not viable.
Clearing	Automatic, sonusDBaasCertificateClearNotification

sonusDBaasCertificateClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.136
Description	Clear alarm for sonusDBaasCertificateNotification
Repetition	No
Event Codes	sonusHostID —The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Instance Fields	sonusHostID, sonusEventDescription, sonusEventClass, sonusEventLevel, sonusEventTime
Action	None
Impact	None
Clearing	Automatic

sonusDBaasReplicationLagNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.137
Description	Replication lag notification.

Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	sonusEventDescription
Action	1. Navigate to <code>/etc/sonus/RDSyncStatus.sh</code> 2. Check the network latency within the EMS node cluster.
Impact	The database is down or the I/O operation speed is slow.
Clearing	Automatic, sonusDBaaSReplicationLagClearNotification

sonusDBaaSReplicationLagClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.138
Description	This is a clearing alarm for sonusDBaaSReplicationLagNotification .
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	sonusEventDescription
Action	None

Impact	None
Clearing	None

sonusDBaaSDownstreamNodesConnectedNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.139
Description	Downstream nodes connected notification.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	sonusEventDescription
Action	1. Navigate to <code>/etc/sonus/RDSyncStatus.sh</code>. 2. Check if the DB on the standby node is up and running and connectivity is working.
Impact	The standby database is down. If this is the active node, the DB replication is stopped since the standby DB is not reachable. If this is a standby node, then it is not an option.
Clearing	Automatic, sonusDBaaSDownstreamNodesConnectedClearNotification .

sonusDBaaSDownstreamNodesConnectedClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.140

Description	This is the clearing alarm for sonusDBaaSDownstreamNodesConnectedNotification .
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	sonusEventDescription
Action	None
Impact	None
Clearing	None

sonusDBaaSInactiveReplicationSlotsNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.141
Description	Inactive replication slots notification.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	sonusEventDescription

Action	1. Check the status of the standby and try to restore the service. 2. Check network service.
Impact	If this is the active node, then the standby is not being replicated. It is not applicable on the standby node.
Clearing	Automatic, sonusDBaaSInactiveReplicationSlotsClearNotification

sonusDBaaSInactiveReplicationSlotsClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.142
Description	This is the clearing alarm for sonusDBaaSInactiveReplicationSlotsNotification .
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	sonusEventDescription
Action	None
Impact	None
Clearing	None

Device Management Alarms

Contents

- [sonusEmsUpgradeJobFailedErrorNotification](#)
- [sonusEmsBackupJobFailedErrorNotification](#)
- [sonusEmsConfigurationJobFailedErrorNotification](#)
- [sonusEmsRestoreFailedErrorNotification](#)
- [sonusEmsPartialConfigurationJobFailedErrorNotification](#)
- [sonusEmsV2NodeCfgDoneNotification](#)
- [sonusEmsV2NodeCfgFailNotification](#)
- [sonusEmsV2NodeCfgPartialNotification](#)
- [sonusEmsFingerprintChangeNotification](#)
- [sonusEmsFingerprintMismatchNotification](#)

This section covers alarms related to device management.

sonusEmsUpgradeJobFailedErrorNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.89
Description	This alarm indicates SBC management Upgrade schedule failed. The Ribbon Application Management Platform will raise this alarm on SBC 1000/2000 Upgrade operation failure.
Repetition	No
Event Codes	None
Instance Fields	Node, Alarm Name, scheduleId.
Action	Re-execute the upgrade job for failed devices.
Impact	Upgrade for one or more devices failed as part SBC upgrade Job.
Clearing	Manual

sonusEmsBackupJobFailedErrorNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.90
Description	This alarm indicates SBC management Backup schedule failed. The Ribbon Application Management Platform will raise this alarm on an SBC Edge Backup operation failure.

Repetition	No
Event Codes	None
Instance Fields	Node, Alarm Name, scheduleId.
Action	Re-execute the backup job for failed devices.
Impact	Backup for one or more devices failed as part SBC upgrade Job.
Clearing	Manual

sonusEmsConfigurationJobFailedErrorNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.91
Description	This alarm indicates the SBC management Configuration schedule failed. The Ribbon Application Management Platform raises this alarm on a SBC 1000/2000 configuration operation failure.
Repetition	No
Event Codes	None
Instance Fields	Node, Alarm Name, scheduleId.
Action	Re-execute the configuration job for the failed devices.
Impact	The configuration for one or more devices failed as part of the SBC configuration Job.
Clearing	Manual

sonusEmsRestoreFailedErrorNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.92
Description	This alarm reports an SBC management Restore operation failure. The Ribbon Application Management Platform raises this alarm on an SBC 1000/2000 Restore operation failure.

Repetition	No
Event Codes	None
Instance Fields	Node, Alarm Name, scheduleId.
Action	Re-execute the operation for the failed device.
Impact	Restore operation failed for a specific device.
Clearing	Manual

sonusEmsPartialConfigurationJobFailedErrorNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.94
Description	This alarm indicates the SBC Core management Partial Configuration schedule failed.
Repetition	No
Event Codes	None
Instance Fields	• sysName, • sysObjectID, • sonusEventTime, • sonusEventDescription, • sonusEventClass, • sonusEventLevel, • scheduleId, • scheduleName, • failedNodes
Action	Re-execute the Partial Configuration job for the failed devices.
Impact	Partial Configuration for one or more SBC Core devices failed as part of the SBC Configuration Job.
Clearing	Manual

sonusEmsV2NodeCfgDoneNotification

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.57
Description	Successfully configured the specified node.
Repetition	Yes. The registration code maintains the specified host's last state. If the state changes to 'success', an alarm is generated.
Event Codes	sonusEmsNodeid—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	sonusEmsNodeid
Action	None required.
Impact	None.
Clearing	Automatic, clears in 2 minutes

sonusEmsV2NodeCfgFailNotification

This alarm is raised on the device not on the Ribbon Application Management Platform (RAMP).

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.56
Description	RAMP failed to complete PIF collection for the specified node.
Repetition	Yes. The registration code maintains the specified host's last state. If the state changes to 'fail', an alarm is generated.
Event Codes	sonusEmsNodeId—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	sonusEmsNodeId
Action	The action to take for this fault depends upon what version and device RAMP is communicating with when this fault occurs. Please refer to matrix of versions/devices and recommended actions to take when troubleshooting. Also, verify connectivity to the device in question via ping or similar tool that uses same protocol the RAMP uses to configure the device.
Impact	RAMP cannot manage the affected node.
Clearing	Automatic, sonusEmsV2NodeCfgDoneNotification

sonusEmsV2NodeCfgPartialNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.61
Description	The Ribbon Application Management Platform (RAMP) partially configured the specified node. One of the hosts of a redundant configuration was not successfully configured.
Repetition	Yes. The registration code maintains the specified host's last state. If the state changes to 'partial', an alarm is generated. Note that 'partial' indicates that one node in a redundancy setup is not configured correctly
Event Codes	sonusEmsNodeId—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	None.
Action	Do the following: 1. Verify connectivity between the RAMP and the hosts defined for this node. 2. Verify that the Sonus agent is running on each of the hosts.
Impact	The node for which the configuration is incomplete may not be manageable by RAMP.
Clearing	Automatic, sonusEmsV2NodeCfgDoneNotification

sonusEmsFingerprintChangeNotification

Type: **CRITICAL**

OID	1.3.6.1.4.1.2879.2.1.7.2.0.122
Description	The alarm is raised if the fingerprint changes on the device.
Repetition	No, the Ribbon Application Management Platform (RAMP) raises the alarm during device discovery.
Event Codes	• sonusEventTime: Provides timestamp of when the event occurs. • sonusEventDescription: Describes the event. • sonusEventClass: Lists the associated event class. • sonusEventLevel: Lists the associated event level (severity).
Instance Fields	• sysName • sysObjectID • sonusEventTime • sonusEventDescription • sonusEventClass • sonusEventLevel
Action	Check whether the fingerprint on the device changed. If the fingerprint displayed in the alarm is not identical to the device, verify the fingerprint manually. If the fingerprints do not match, unregister and reregister the device.
Impact	• Possible case of man-in-the-middle attack An attacker tries to intercept the communication between the RAMP and the device. The device is compromised. • A normal notification on fingerprint change The fingerprint of the device genuinely changed. No impact.
Clearing	Manual

sonusEmsFingerprintMismatchNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.123
Description	The alarm is raised if fingerprint verification fails on the device.
Repetition	None
Event Codes	• sonusEventTime: Provides timestamp of when the event occurs. • sonusEventDescription: Describes the event. • sonusEventClass: Lists the associated event class. • sonusEventLevel: Lists the associated event level (severity).

Instance Fields	• sysName • sysObjectID • sysName • sysObjectID • sonusEventTime • sonusEventDescription • sonusEventClass • sonusEventLevel
Action	Check whether the fingerprint on the connecting device changed. If the fingerprint changed, discover the device again.
Impact	The Ribbon Application Management Platform tries to establish a connection with an attacker.
Clearing	Manual

EdgeMarc Alarms

In this section:

- [EdgeMarc:ribbonApplicationDiagnosticReport](#)
- [EdgeMarc:ribbonDeviceDown](#)
- [EdgeMarc:ribbonDeviceUp](#)
- [EdgeMarc:ribbonKernelDiagnosticReport](#)
- [EdgeMarc:ribbonLANStatusDown](#)
- [EdgeMarc:ribbonMOSBelowThreshold](#)
- [EdgeMarc:ribbonSIPServerChange](#)
- [EdgeMarc:ribbonSIPServerModeChange](#)
- [EdgeMarc:ribbonSIPServerUnavailable](#)
- [EdgeMarc:ribbonT1StatusDown](#)
- [EdgeMarc:ribbonWANLinkChange](#)

EdgeMarc:ribbonApplicationDiagnosticReport

Type: User-specified

OID	1.3.6.1.4.1.2879.2.1.20.2.1.10

Description	This event is generated when any application crashes on the Edgemarc device.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level. sonusEventTime: The timestamp of the event.
Instance Fields	None
Action	Check the diagnostic files generated by the event.
Impact	No impact on RAMP.
Clearing	No

EdgeMarc:ribbonDeviceDown

Type: User-specified

OID	1.3.6.1.4.1.2879.2.1.20.2.1.1
Description	If the Device Down rule is configured for an EdgeMarc device or a resource group, and if the connection between the RAMP and the device gets disconnected, then the ribbonDeviceDown alarm is raised.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level. sonusEventTime: The timestamp of the event.
Instance Fields	None
Action	The only action for this rule is notifying recipients.
Impact	You cannot perform operations on the EdgeMarc device.
Clearing	Manual, EdgeMarc:ribbonDeviceUp

EdgeMarc:ribbonDeviceUp

Type: User-specified

OID	1.3.6.1.4.1.2879.2.1.20.2.1.2
Description	If the Device Up rule is configured for an EdgeMarc device or a resource group, and if the connection between the RAMP and the device is re-established, then the ribbonDeviceUp alarm is raised.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level. sonusEventTime: The timestamp of the event.
Instance Fields	None
Action	The only action for this rule is notifying recipients.
Impact	None
Clearing	N/A

EdgeMarc:ribbonKernelDiagnosticReport

Type: User-specified

OID	1.3.6.1.4.1.2879.2.1.20.2.1.11
Description	This event is generated when the kernel crashes on an EdgeMarc device.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level. sonusEventTime: The timestamp of the event.
Instance Fields	None

Action	Check the diagnostic file generated by the event.
Impact	The EdgeMarc device remains in an offline state until the kernel restarts on the EdgeMarc device. You cannot perform any operations on the device until it is online.
Clearing	N/A

EdgeMarc:ribbonLANStatusDown

Type: User-specified

OID	1.3.6.1.4.1.2879.2.1.20.2.1.8
Description	If the LAN Status Down rule is configured for an EdgeMarc device or a resource group and if the LAN interface goes down on the EdgeMarc device then the ribbonLANStatusDown alarm is raised.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level. sonusEventTime: The timestamp of the event.
Instance Fields	None
Action	The only action for this rule is notifying recipients.
Impact	No impact on RAMP.
Clearing	N/A

EdgeMarc:ribbonMOSBelowThreshold

Type: User-specified

OID	1.3.6.1.4.1.2879.2.1.20.2.1.3
Description	If MOS score falls below pre-configured threshold on an individual device.
Repetition	No

Event Codes	sonusHostID: The unique ID or serial number for this host. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level. sonusEventTime: The timestamp of the event.
Instance Fields	ribbonMOSBelowThersholdCount: The number of occurrences per device when MOS is below threshold. ribbonMOSBelowThresholdMinutes : Duration in minutes to count the MOS below threshold.
Action	Retrieve Ring Buffer contents for the time period.
Impact	No impact on RAMP.
Clearing	N/A

EdgeMarc:ribbonSIPServerChange

Type: User-specified

OID	1.3.6.1.4.1.2879.2.1.20.2.1.6
Description	If the SIP Server Change rule is configured for an EdgeMarc device or a resource group, and if the SIP server changes for the EdgeMarc device, then the ribbonSIPServerChange alarm is raised.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level. sonusEventTime: The timestamp of the event.
Instance Fields	ribbonSIPServerState : SIP Server State ("Up Down Unknown")
Action	Retrieve Ring Buffer contents for the time period.
Impact	No impact on RAMP. SIP Calls may be affected due to the server change.
Clearing	N/A

EdgeMarc:ribbonSIPServerModeChange

Type: User-specified

OID	1.3.6.1.4.1.2879.2.1.20.2.1.5
Description	If the SIP Server Mode Change rule is configured for an EdgeMarc device or a resource group, and if the SIP server mode changes for the EdgeMarc device, then the ribbonSIPServerModeChange alarm is raised.
Repetition	No
Event Codes	sonusHostID : The unique ID or serial number for this host. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level. sonusEventTime: The timestamp of the event.
Instance Fields	ribbonSIPServerMode: SIP Server Mode ("Up Down Unknown")
Action	Retrieve Ring Buffer contents for the time period.
Impact	No impact on RAMP.
Clearing	N/A

EdgeMarc:ribbonSIPServerUnavailable

Type: User-specified

OID	1.3.6.1.4.1.2879.2.1.20.2.1.4
Description	If the SIP Server Unavailable rule is configured for an EdgeMarc device or a resource group, then whenever the SIP server goes offline and is unavailable for the EdgeMarc device then the ribbonSIPServerUnavailable alarm is raised.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level. sonusEventTime: The timestamp of the event.
Instance Fields	None
Action	Retrieve Ring Buffer contents for the time period.

Impact	No impact on RAMP. SIP calls will be affected as the server is unavailable.
Clearing	N/A

EdgeMarc:ribbonT1StatusDown

Type: User-specified

OID	1.3.6.1.4.1.2879.2.1.20.2.1.9
Description	If the T1 Status Down rule is configured for an EdgeMarc device or a resource group, and if the T1 interface is down on the EdgeMarc device then the ribbonT1tatusDown alarm is raised.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for this host. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level. sonusEventTime: The timestamp of the event.
Instance Fields	None
Action	The only action for this rule is notifying recipients.
Impact	No impact on RAMP.
Clearing	N/A

EdgeMarc:ribbonWANLinkChange

Type: User-specified

OID	1.3.6.1.4.1.2879.2.1.20.2.1.7
Description	If the WAN Link Change rule is configured for an EdgeMarc device or a resource group, and if the connectivity switches from a WAN interface to another interface on an EdgeMarc device then the ribbonWANLinkChange alarm is raised.
Repetition	No

Event Codes	sonusHostID: The unique ID or serial number for this host. sonusEventDescription: The description of the event. sonusEventClass: The event class. sonusEventLevel: The event level. sonusEventTime: The timestamp of the event.
Instance Fields	ribbonWANLinkState: WAN Link State ("Up Down Unknown")
Action	Retrieve Ring Buffer contents for the time period.
Impact	The EdgeMarc device is offline for a few minutes. You cannot perform any operations on an EdgeMarc device if it is in an offline state.
Clearing	N/A

GSX Discovery

In this section:

- [sonusEmsV2PifCollectDoneNotification](#)
- [sonusEmsV2PifCollectFailNotification](#)

sonusEmsV2PifCollectDoneNotification

This alarm is raised on the device not on the Ribbon Application Management Platform (RAMP).

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.78
Description	This notification indicates that the PIF was processed successfully for the specified GSX node <nodeId>.
Repetition	Yes. Repeats each time PIF collection succeeds.

Event Codes	sonusEmsNodeId—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	sonusEmsNodeId
Action	None required. Any accumulated sonusEmsV2PifCollectFailNotification alarms are automatically cleared.
Impact	None.
Clearing	Automatic, clears in two minutes

sonusEmsV2PifCollectFailNotification

This alarm is raised on the device not on the Ribbon Application Management Platform (RAMP).

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.77
Description	This notification occurs under two conditions: 1. COPY Error – A PIF file is not copied from DSI to RAMP for the specified GSX node (nodeID). 2. PROCESS Error – A PIF file is not processed by the RAMP for the specified GSX node (nodeID).
Repetition	Yes. Repeats each time PIF collection fails.

Event Codes	sonusEmsNodeId—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining `what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	sonusEmsNodeId
Action	Take appropriate action: COPY Error 1. If agent is configured to copy the PIF file, verify that the agent is running. 2. If DSI file system is mounted for file copying, verify that the file system is mounted correctly and is not stale. PROCESS Error 1. If PIF file is corrupted, ensure the PIF file is generated by the released GSX images. 2. If data failed to load from <code>ctl</code> and <code>dat</code> files to database, ensure <code>oracle_home</code> is defined correctly under Oracle account.
Impact	Many RAMP features (Trunk Group reports, Trunk Group wizards, Traffic Management provisioning, etc.) rely on PIF data that is collected and loaded into the database. When PIF data collection ceases, the associated RAMP feature(s), when used, are accessing out-of-date information from the database.
Clearing	Automatic, sonusEmsV2PifCollectDoneNotification

High Availability Alarms

The alarms listed in this section are the PSX High Availability (HA) alarms.

In this section:

- [sonusHAConnectToPeerFailureExtendedNotification](#)
- [sonusHAConnectToPeerSuccessExtendedNotification](#)
- [sonusHAFailoverInitiatedNotification](#)
- [sonusHAHeartBeatFailureNotification](#)
- [sonusHAResourceAcquireFailureNotification](#)
- [sonusHAResourceReleaseFailureNotification](#)
- [sonusHAStateChangeNotification](#)

sonusHAConnectToPeerFailureExtendedNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.5.17.2.0.8
Description	Failure to connect to peer.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters. sonusHAPeerExtendedIpType: The IP type (IPv4 or IPv6). sonusHAPeerExtendedIpAddress: IPv4 or IPv6 Address of the Softswitch (required parameter). sonusHAPeerExtendedIpAddressType: IP Address type of the Softswitch (required parameter). sonusHACurrentState: The present high availability state of this host. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	sonusHAPeerExtendedIpAddress
Action	Investigate to determine why the system cannot connect to the peer. Validate the following conditions: - Network connections - Network routing - Configured peer IP addresses
Impact	If the number of retries exceeds a configurable parameter named "Number of Retries Before Assert," the system starts the process to become active.

Clearing	Automatic, sonusHAConnectToPeerSuccessExtendedNotification .

sonusHAConnectToPeerSuccessExtendedNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.5.17.2.0.9
Description	Successfully connected to the peer.
Repetition	No
Event Codes	sonusHostID: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters. sonusHAPeerExtendedIpType: The IP type (IPv4 or IPv6). sonusHAPeerExtendedIpAddress: IPv4 or IPv6 Address of the Softswitch (required parameter). sonusHAPeerExtendedIpAddressType: IP Address type of the Softswitch (required parameter). sonusHACurrentState: The present high availability state of this host. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	sonusHAPeerExtendedIpAddress
Action	None
Impact	None
Clearing	Automatic, clears in two minutes.

sonusHAFailoverInitiatedNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.5.17.2.0.1
Description	The HA failover process is initiated.
Repetition	Yes. Repeats each time a failover is initiated.
Event Codes	sonusHAFailoverReason: The reason for failover. sonusHostID: The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	None
Action	If the alarm is initiated by an operator, then no action is needed. Else, investigate the reason for the failover and take corrective action. This trap is cleared by the transition of sonusHAStateChange to active state.
Impact	During failover, the clients will lose connectivity for a few minutes until the new active system is fully operational.
Clearing	Automatic, sonusHAStateChangeNotification , (state change = active(1)).

sonusHAHeartBeatFailureNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.5.17.2.0.7
Description	The peer did not respond to the heartbeat request.
Repetition	Yes. Repeats each time a heartbeat failure occurs.

Event Codes	sonusHAResource: The resource values like database, disk, network, and wellknownip. sonusHostID: The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	None
Action	The probable cause of failure is related problems. Validate the following conditions: - Network connections - Network routing - Configured peer IP addresses
Impact	If the number of keep-alive missed messages exceeds a configurable parameter (Keep Alive Retries), the system starts the process to become active.
Clearing	Automatic, clears in three minutes.

sonusHAResourceAcquireFailureNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.5.17.2.0.5
Description	The HA component was unable to acquire the specified resource during a failover procedure.
Repetition	Yes. Repeats each time an attempt to acquire the specified resource fails.

Event Codes	sonusHAResource: The resource values like, database, disk, network, and wellknownlp. sonusHostID: The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	sonusHostID
Action	Find the events surrounding the attempt by the resource to become active, and take corrective action. Contact Ribbon Support for assistance.
Impact	The identified resource is down. When a system tries to acquire resources, it is attempting to become active. Hence, when an acquire operation fails, the system cannot become active.
Clearing	Automatic, sonusHAStateChangeNotification , (state change = active(1)).

sonusHAResourceReleaseFailureNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.5.17.2.0.6
Description	The HA component is unable to release the specified resource during a failover procedure.
Repetition	Yes. Repeats each time an attempt to release the specified resource fails.

Event Codes	sonusHostID: The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.
Instance Fields	sonusHostID
Action	Find the events surrounding the attempt by the resource to become active, and take corrective action. Contact Ribbon Support for assistance.
Impact	The identified resource is down. When a system is unable to release resources, its peer cannot acquire the resources. As a result, the peer cannot become active and it will also be down.
Clearing	Automatic, sonusHAStateChangeNotification , (state change = active(1)).

sonusHAStateChangeNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.5.17.2.0.4
Description	The host's HA state has changed.
Repetition	Yes. Repeats each time the HA state changes for the specified host.
Event Codes	sonusHAPrevState: The previous high availability state of this host. sonusHANewState: The new high availability state of this host. sonusHostID: The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusEventTime: Provides the timestamp of when the event occurs.

Instance Fields	sonusHANewState
Action	If the alarm is initiated by an operator, then no action is needed. Else, investigate the event and take corrective action. Look for a prior trap that may have triggered this state change trap, and resolve this failure.
Impact	A change of state during a system startup is normal. But a state change while a system is running is a cause for concern. This may indicate a failover is taking place.
Clearing	Automatic, sonusHANewState = active(1).

Licensing Management Alarms

Contents

- [sonusLicExpiredNotification](#)
- [sonusLicStatusNotification](#)
- [sonusLicUsageExceededNotification](#)
- [sonusLicUsageStatusNotification](#)
- [sonusLicSBCLicMismatchNotification](#)
- [sonusLicSBCLicMismatchClearNotification](#)
- [sonusLicFailedToSendUsageFileNotification](#)
- [sonusLicFailedToRegisterWithITNotification](#)
- [sonusLicDeviceRegisterFailedNotification](#)
- [sonusLicStatusClearNotification](#)
- [sonusLicPostPaidReportGenFailNotification](#)
- [sonusLicPostPaidReportGenFailClearNotification](#)
- [sonusLicProfileAssociationFailNotification](#)

This section covers alarms related to license management.

sonusLicExpiredNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.1
Description	A license identified by the tuple sonusTargetType, sonusTargetId, sonusFeatureId has expired as of sonusLicExpireTime.

Repetition	No.
Event Codes	sonusLicExpireTime —The date/time when the license expires. sonusLicFeatureId —The license feature identifier. sonusLicTargetId —The license target identifier. sonusLicTargetType —The license target type.
Instance Fields	sonusLicTargetType, sonusLicTargetId, sonusLicFeatureId
Action	Contact Ribbon account team for a new license, if required.
Impact	The associated feature is disabled on the target device.
Clearing	Manual.

sonusLicStatusNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.2
Description	This notification is sent when a license is about to expire.
Repetition	No.
Event Codes	sonusLicExpireTime —The date/time when the license expires. sonusLicFeatureId —The license feature identifier. sonusLicTargetId —The license target identifier. sonusLicTargetType —The license target type.
Instance Fields	sonusLicTargetId
Action	Contact Ribbon account team for a new license, if required.
Impact	The license for the specified feature is approaching expiration; the target device will disable the feature once the license expires.
Clearing	Automatic, sonusLicStatusClearNotification .

sonusLicUsageExceededNotification

Note

The sonusLicUsageExceededNotification trap only applies to Node-Locked licenses.

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.3
Description	The current usage (sonusLicPresentValue) for the license identified by the tuple (sonusTargetType, sonusTargetId, sonusFeatureId) exceeded the configured maximum value (sonusLicConfiguredValue).
Repetition	Yes. Repeats every 15 minutes as long as sonusLicPresentValue exceeds maximum value of sonusLicConfiguredValue.
Event Codes	sonusLicConfiguredValue —The current configured maximum usage. sonusLicFeatureId —The license feature identifier. sonusLicPresentValue —The current license usage. sonusLicTargetId —The license target identifier. sonusLicTargetType —The license target type.
Instance Fields	sonusLicTargetType, sonusLicTargetId, sonusLicFeatureId
Action	Contact your Ribbon account representative to obtain a new license to increase the license usage limit.
Impact	The target device may reject further provisioning of the specified feature since the maximum usage limit is exceeded.
Clearing	Manual.

sonusLicUsageStatusNotification**Type: CRITICAL**

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.4
Description	Current usage, sonusLicPresentValue, for the license identified by the tuple sonusTargetType, sonusTargetId, sonusFeatureId is approaching the configured maximum value of sonusLicConfiguredValue.
Repetition	Yes. Repeats every 15 minutes as long as sonusLicPresentValue is within the prescribed range of maximum value of sonusLicConfiguredValue.

Event Codes	sonusLicConfiguredValue —The current configured maximum usage. sonusLicFeatureId —The license feature identifier. sonusLicPresentValue —The current license usage. sonusLicTargetId —The license target identifier. sonusLicTargetType —The license target type.
Instance Fields	sonusLicTargetType, sonusLicTargetId, sonusLicFeatureId
Action	Contact Ribbon account team for a new license to increase usage limit.
Impact	The maximum usage limit is about to be reached. The target device may reject further provisioning of the specified feature once the limit is reached.
Clearing	Manual.

sonusLicSBCLicMismatchNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.7
Description	The alarm is raised if the count of SBC-RTU and SBC-POL-RTU licenses are not equal after the licenses are installed.
Repetition	Yes
Event Codes	sonusEventTime : Provides timestamp of when the event occurs. sonusEventDescription : Describes the event. sonusEventClass : Lists the associated event class. sonusEventLevel : Lists the associated event level (severity). sonusLicTargetType : The license target type.
Instance Fields	sonusEventTime sonusEventDescription, sonusEventClass sonusEventLevel sonusLicTargetType
Action	Manual
Impact	No impact on the Ribbon Application Management Platform.

Clearing	Automatic, sonusLicSBCLicMismatchClearNotification

sonusLicSBCLicMismatchClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.8
Description	This notification occurs when the license count is of SBC-RTU and SBC-POL-RTU is same.
Repetition	Yes
Event Codes	sonusEventTime: Provides timestamp of when the event occurs. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusLicTargetType: The license target type.
Instance Fields	sonusEventTime sonusEventDescription sonusEventClass sonusEventLevel sonusLicTargetType
Action	None
Impact	No impact on the Ribbon Application Management Platform.
Clearing	Automatic

sonusLicFailedToSendUsageFileNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.9
Description	This alarm is raised when the Ribbon Application Management Platform (RAMP) fails to send the auto-generated post-paid license usage file.
Repetition	None

Event Codes	sonusEventTime: Provides timestamp of when the event occurs. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusLicPPDFFileName: The license PDF file name.
Instance Fields	sonusEventTime sonusEventDescription sonusEventClass sonusEventLevel sonusLicPPDFFileName
Action	Check whether the URL for IT is reachable from RAMP.
Impact	Auto-generated post-paid license reports are not sent to IT.
Clearing	Manual

sonusLicFailedToRegisterWithITNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.10
Description	This alarm is raised when the Ribbon Application Management Platform (RAMP) fails to register with IT.
Repetition	None
Event Codes	sonusEventTime: Provides timestamp of when the event occurs. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity).
Instance Fields	sonusEventTime sonusEventDescription sonusEventClass sonusEventLevel
Action	Check whether the URL for IT is reachable from RAMP.
Impact	Auto-generated post-paid license reports will not be sent to IT.

Clearing	Manual

sonusLicDeviceRegisterFailedNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.12
Description	Devices whose licenses are managed by Ribbon Application Management Platform (RAMP) must periodically register with the License Manager (LM) service. The registration fails and LM responds with an error response if there are no usage level statistics from the device for the last 90 days.
Repetition	Repeats when the SBC sends another registration request to the LM.
Event Codes	sonusEventTime, sonusEventDescription, sonusEventClass, sonusEventLevel, sonusLicTargetId, sonusLicTargetType, sonusLicPresentValue, sonusLicConfiguredValue
Instance Fields	None
Action	The LM service sends a failed response to the SBC along with the last collection epoch time, once the RAMP threshold is reached.
Impact	The SBC cannot register with the LM service, therefore the SBC license grace period is started.
Clearing	Manual

sonusLicStatusClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.5
Description	This notification is sent when a license is renewed.
Repetition	Yes. This notification is sent every-time a license is renewed.

Event Codes	sonusEventTime : Provides timestamp of when the event occurs. sonusEventDescription : Describes the event. sonusEventClass : Lists the associated event class. sonusEventLevel : Lists the associated event level (severity).
Instance Fields	sonusLicTargetId : The license target identifier.
Action	None
Impact	The license validity is extended. The associated feature can be used till the renewed validity date.
Clearing	Automatic

sonusLicPostPaidReportGenFailNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.13
Description	This alarm is raised if the postpaid report was not auto generated for the previous day.
Repetition	Yes. Once every day.
Event Codes	sonusEventTime : Provides timestamp of when the event occurs. sonusEventDescription : Describes the event. sonusEventClass : Lists the associated event class. sonusEventLevel : Lists the associated event level (severity). sonusLicTargetType : The license target type.
Instance Fields	sonusLicTargetType
Action	Manual. Check for the reason of this alarm.
Impact	Postpaid reports are not available to share with Ribbon. So billing is affected.
Clearing	Automatic, sonusLicPostPaidReportGenFailClearNotification

sonusLicPostPaidReportGenFailClearNotification**Type: CLEAR**

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.14
Description	This alarm is raised after postpaid report auto-generation resumes.
Repetition	No
Event Codes	sonusEventTime: Provides timestamp of when the event occurs. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusLicTargetType: The license target type.
Instance Fields	sonusLicTargetType
Action	None
Impact	Postpaid reports are available to share with Ribbon.
Clearing	Automatic.

sonusLicProfileAssociationFailNotification**Type: MAJOR**

OID	1.3.6.1.4.1.2879.2.1.7.3.2.0.15
Description	This alarm is raised if License Profile Association Fails.
Repetition	No

Event Codes	sonusEventTime: Provides timestamp of when the event occurs. sonusEventDescription: Describes the event. sonusEventClass: Lists the associated event class. sonusEventLevel: Lists the associated event level (severity). sonusLicTargetType: The license target type.
Instance Fields	sonusLicTargetType
Action	Manual, check for the reason of this alarm.
Impact	No impact on the Ribbon Application Management Platform.
Clearing	Manual

Normalized Alarms

In this section:

- [GVAlarmCritical](#)
- [GVAlarmMajor](#)
- [GVAlarmMinor](#)
- [GVAlarmWarning](#)
- [GVAlarmClear](#)
- [GVFaultMessage](#)

The normalized alarm forwarding interface supports the following standard alarms. All the received network element alarms are mapped to one of the standard alarms based on the severity.

Attribute	Description	OID
GVAlarmCritical	Maps to all Insight Critical alarms.	.1.3.6.1.4.1.5584.2.3.0.1
GVAlarmMajor	Maps to all Insight Major alarms.	.1.3.6.1.4.1.5584.2.3.0.2
GVAlarmMinor	Maps to all Insight Minor alarms.	.1.3.6.1.4.1.5584.2.3.0.3
GVAlarmWarning	Maps to all Insight Warning alarms.	.1.3.6.1.4.1.5584.2.3.0.4

Attribute	Description	OID
GVAlarmClear	Maps to all Insight Clear alarms.	.1.3.6.1.4.1.5584.2.3.0.5
GVFaultMessage	Maps to all Insight non-fault events.	.1.3.6.1.4.1.5584.2.3.0.6

GVAlarmCritical

Note

All the Critical alarms (irrespective of node types) are forwarded to the upstream OSS system with the alarm name as "GVAlarmCritical."

Before forwarding, all the attributes of the original alarm are mapped to the attributes mentioned.

Normalized alarm supports the following attributes.

Alarm attributes

Attribute	Type	OID	Description
alarmActiveIndex	Counter64	.1.3.6.1.4.1.5584.2.3.3.1.1	A running counter that uniquely identifies every alarm and acts as a correlation identifier for upstream OSS system. It supports the following correlations: - duplicate alarms - the same identifier is used for duplicate alarms. - clear alarms - the same identifier is used for raise and clearing alarms.
gvAlarmEventTy e	IANAItuEventType Types of gvAlarmEventType: communicationsAlar m, qualityOfServiceAlar m, processingErrorAlar m, equipmentAlarm, environmentalAlarm.	.1.3.6.1.4.1.5584.2.3.3.1.4	The event type as described in IANA-ITU-ALARM-TC-MIB.

Attribute	Type	OID	Description
gvAlarmProbableCause	IANAItuProbableCause	.1.3.6.1.4.1.5584.2.3.3.1.5	The probable cause of the event as described in IANA-ITU-ALARM-TC-MIB.
gvAlarmComponentID	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.7	The string contains host name and fully distinguished name of sub-component under alarm. It maps to Event Code(s) and Instance Fields as name value pairs in the format – "TYPE=SBC, HOST=[host name], COMPONENT=[component name]. The TYPE and HOST strings are derived from the Ribbon Application Management Platform node attributes that are received during node registration. The Component string is derived as comma separated key value pairs; where the keys are Event Code(s)/Instance fields with the corresponding values received from the agent that generated the alarm.
gvAlarmAdditionalText	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.10	The Definition, Impact, Recommended Action, and Repetition as name value pairs.
alarmActiveDateAndTime	DateAndTime	.1.3.6.1.4.1.5584.2.3.3.1.2	The timestamp of the the event.
alarmActiveDescription	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.3	The description of the event.
gvAlarmEventTypeString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.12	The event type. If a device event type value is not found in IANA scheme and a custom text is included for for event type.
gvAlarmCauseString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.11	The cause of the event. If a device has not found a cause value in IANA scheme it includes a text value for cause.
gvAlarmName	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.6	The original alarm name from the node.

Attribute	Type	OID	Description
gvAlarmManualClear	INTEGER	.1.3.6.1.4.1.5584.2.3.3.1.8	Specifies whether alarm clearing is manual or automatic. • 2 indicates automatic clearing. • 3 indicates manual clearing.

GVAlarmMajor

Note

All the Major alarms (irrespective of node types) are forwarded to the upstream OSS system with the alarm name as "GVAlarmMajor."

Before forwarding, all the attributes of the original alarm are mapped to the attributes mentioned.

Normalized alarm supports the following attributes.

Alarm attributes

Attribute	Type	OID	Description
alarmActiveIndex	Counter64	.1.3.6.1.4.1.5584.2.3.3.1.1	A running counter that uniquely identifies every alarm and acts as a correlation identifier for upstream OSS system. It supports the following correlations: • duplicate alarms - the same identifier is used for duplicate alarms. • clear alarms - the same identifier is used for raise and clearing alarms.
gvAlarmEventType	IANAItuEventType Types of gvAlarmEventType: communicationsAlarm, qualityOfServiceAlarm, processingErrorAlarm, equipmentAlarm, environmentalAlarm.	.1.3.6.1.4.1.5584.2.3.3.1.4	The event type as described in IANA-ITU-ALARM-TC-MIB.

Attribute	Type	OID	Description
gvAlarmProbableCause	IANAItuProbableCause	.1.3.6.1.4.1.5584.2.3.3.1.5	The probable cause of the event as described in IANA-ITU-ALARM-TC-MIB.
gvAlarmComponentID	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.7	The string contains host name and fully distinguished name of sub-component under alarm. It maps to Event Code(s) and Instance Fields as name value pairs in the format – "TYPE=SBC, HOST=[host name], COMPONENT=[component name]. The TYPE and HOST strings are derived from the Ribbon Application Management Platform node attributes that are received during node registration. The Component string is derived as comma separated key value pairs; where the keys are Event Code(s)/Instance fields with the corresponding values received from the agent that generated the alarm.
gvAlarmAdditionalText	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.10	The Definition, Impact, Recommended Action, and Repetition as name value pairs.
alarmActiveDateAndTime	DateAndTime	.1.3.6.1.4.1.5584.2.3.3.1.2	The timestamp of the the event.
alarmActiveDescription	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.3	The description of the event.
gvAlarmEventTypeString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.12	The event type. If a device event type value is not found in IANA scheme and a custom text is included for for event type.
gvAlarmCauseString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.11	The cause of the event. If device has not found a cause value in IANA scheme then this include a text value for cause.
gvAlarmName	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.6	The original alarm name from the node.

Attribute	Type	OID	Description
gvAlarmManualClear	INTEGER	.1.3.6.1.4.1.5584.2.3.3.1.8	Specifies whether alarm clearing is manual or automatic. • 2 indicates automatic clearing. • 3 indicates manual clearing.

GVAlarmMinor

Note

All the Minor alarms (irrespective of node types) are forwarded to the upstream OSS system with the alarm name as "GVAlarmMinor."

Before forwarding, all the attributes of the original alarm are mapped to the attributes mentioned.

Normalized alarm supports the following attributes.

Alarm attributes

Attribute	Type	OID	Description
alarmActiveIndex	Counter64	.1.3.6.1.4.1.5584.2.3.3.1.1	A running counter that uniquely identifies every alarm and acts as a correlation identifier for upstream OSS system. It supports the following correlations: • duplicate alarms - the same identifier is used for duplicate alarms. • clear alarms - the same identifier is used for raise and clearing alarms.
gvAlarmEventType	IANAItuEventType Types of gvAlarmEventType: communicationsAlarm, qualityOfServiceAlarm, processingErrorAlarm, equipmentAlarm, environmentalAlarm.	.1.3.6.1.4.1.5584.2.3.3.1.4	The event type as described in IANA-ITU-ALARM-TC-MIB.

Attribute	Type	OID	Description
gvAlarmProbableCause	IANAItuProbableCause	.1.3.6.1.4.1.5584.2.3.3.1.5	The probable cause of the event as described in IANA-ITU-ALARM-TC-MIB.
gvAlarmComponentID	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.7	The string contains host name and fully distinguished name of sub-component under alarm. It maps to Event Code(s) and Instance Fields as name value pairs in the format – "TYPE=SBC, HOST=[host name], COMPONENT=[component name]. The TYPE and HOST strings are derived from the Ribbon Application Management Platform node attributes that are received during node registration. The Component string is derived as comma separated key value pairs; where the keys are Event Code(s)/Instance fields with the corresponding values received from the agent that generated the alarm.
gvAlarmAdditionalText	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.10	The Definition, Impact, Recommended Action, and Repetition as name value pairs.
alarmActiveDateAndTime	DateAndTime	.1.3.6.1.4.1.5584.2.3.3.1.2	The timestamp of the the event.
alarmActiveDescription	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.3	The description of the event.
gvAlarmEventTypeString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.12	The event type. If a device event type value is not found in IANA scheme and a custom text is included for for event type.
gvAlarmCauseString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.11	The cause of the event. If device has not found a cause value in IANA scheme then this include a text value for cause.
gvAlarmName	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.6	The original alarm name from the node.

Attribute	Type	OID	Description
gvAlarmManualClear	INTEGER	.1.3.6.1.4.1.5584.2.3 .3.1.8	Specifies whether alarm clearing is manual or automatic. • 2 indicates automatic clearing. • 3 indicates manual clearing.

GVAlarmWarning

Note

All the Warning alarms (irrespective of node types) are forwarded to the upstream OSS system with the alarm name as "GVAlarmWarning."

Before forwarding, all the attributes of the original alarm are mapped to the attributes mentioned.

Normalized alarm supports the following attributes.

Alarm attributes

Attribute	Type	OID	Description
alarmActiveIndex	Counter64	.1.3.6.1.4.1.5584.2.3 .3.1.1	A running counter that uniquely identifies every alarm and acts as a correlation identifier for upstream OSS system. It supports the following correlations: • duplicate alarms - the same identifier is used for duplicate alarms. • clear alarms - the same identifier is used for raise and clearing alarms.
gvAlarmEventType	IANAItuEventType Types of gvAlarmEventType: communicationsAlarm, qualityOfServiceAlarm, processingErrorAlarm, equipmentAlarm, environmentalAlarm.	.1.3.6.1.4.1.5584.2.3 .3.1.4	The event type as described in IANA-ITU-ALARM-TC-MIB.

Attribute	Type	OID	Description
gvAlarmProbableCause	IANAItuProbableCause	.1.3.6.1.4.1.5584.2.3.3.1.5	The probable cause of the event as described in IANA-ITU-ALARM-TC-MIB.
gvAlarmComponentID	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.7	The string contains host name and fully distinguished name of sub-component under alarm. It maps to Event Code(s) and Instance Fields as name value pairs in the format – "TYPE=SBC, HOST=[host name], COMPONENT=[component name]. The TYPE and HOST strings are derived from the Ribbon Application Management Platform node attributes that are received during node registration. The Component string is derived as comma separated key value pairs; where the keys are Event Code(s)/Instance fields with the corresponding values received from the agent that generated the alarm.
gvAlarmAdditionalText	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.10	The Definition, Impact, Recommended Action, and Repetition as name value pairs.
alarmActiveDateAndTime	DateAndTime	.1.3.6.1.4.1.5584.2.3.3.1.2	The timestamp of the the event.
alarmActiveDescription	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.3	The description of the event.
gvAlarmEventTypeString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.12	The event type. If a device event type value is not found in IANA scheme and a custom text is included for for event type.
gvAlarmCauseString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.11	The cause of the event. If device has not found a cause value in IANA scheme then this include a text value for cause.
gvAlarmName	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.6	The original alarm name from the node.

Attribute	Type	OID	Description
gvAlarmManualClear	INTEGER	.1.3.6.1.4.1.5584.2.3 .3.1.8	Specifies whether alarm clearing is manual or automatic. • 2 indicates automatic clearing. • 3 indicates manual clearing.

GVAlarmClear

Note

All the Clear alarms (irrespective of node types) are forwarded to the upstream OSS system with the alarm name as "GVAlarmClear."

Before forwarding, all the attributes of the original alarm are mapped to the attributes mentioned.

Normalized alarm supports the following attributes.

Alarm attributes

Attribute	Type	OID	Description
alarmActiveIndex	Counter64	.1.3.6.1.4.1.5584.2.3 .3.1.1	A running counter that uniquely identifies every alarm and acts as a correlation identifier for upstream OSS system. It supports the following correlations: • duplicate alarms - the same identifier is used for duplicate alarms. • clear alarms - the same identifier is used for raise and clearing alarms.
gvAlarmEventType	IANAItuEventType Types of gvAlarmEventType: communicationsAlarm, qualityOfServiceAlarm, processingErrorAlarm, equipmentAlarm, environmentalAlarm.	.1.3.6.1.4.1.5584.2.3 .3.1.4	The event type as described in IANA-ITU-ALARM-TC-MIB.

Attribute	Type	OID	Description
gvAlarmProbableCause	IANAItuProbableCause	.1.3.6.1.4.1.5584.2.3.3.1.5	The probable cause of the event as described in IANA-ITU-ALARM-TC-MIB.
gvAlarmComponentID	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.7	The string contains host name and fully distinguished name of sub-component under alarm. It maps to Event Code(s) and Instance Fields as name value pairs in the format – "TYPE=SBC, HOST=[host name], COMPONENT=[component name]. The TYPE and HOST strings are derived from the Ribbon Application Management Platform node attributes that are received during node registration. The Component string is derived as comma separated key value pairs; where the keys are Event Code(s)/Instance fields with the corresponding values received from the agent that generated the alarm.
gvAlarmAdditionalText	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.10	The Definition, Impact, Recommended Action, and Repetition as name value pairs.
alarmActiveDateAndTime	DateAndTime	.1.3.6.1.4.1.5584.2.3.3.1.2	The timestamp of the the event.
alarmActiveDescription	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.3	The description of the event.
gvAlarmEventTypeString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.12	The event type. If a device event type value is not found in IANA scheme and a custom text is included for for event type.
gvAlarmCauseString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.11	The cause of the event. If device has not found a cause value in IANA scheme then this include a text value for cause.
gvAlarmName	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.6	The original alarm name from the node.

Attribute	Type	OID	Description
gvAlarmManualClear	INTEGER	.1.3.6.1.4.1.5584.2.3.3.1.8	Specifies whether alarm clearing is manual or automatic. 2 indicates automatic clearing. 3 indicates manual clearing.

GVFaultMessage

Note

All the Fault Messages (irrespective of node types) are forwarded to the upstream OSS system with the alarm name as "GVAlarmFaultMessage."

Before forwarding, all the attributes of the original alarm are mapped to the attributes mentioned.

Normalized alarm supports the following attributes.

Alarm attributes

Attribute	Type	OID	Description
alarmActiveIndex	Counter64	.1.3.6.1.4.1.5584.2.3.3.1.1	A running counter that uniquely identifies every alarm and acts as a correlation identifier for upstream OSS system. It supports the following correlations: - duplicate alarms - the same identifier is used for duplicate alarms. - clear alarms - the same identifier is used for raise and clearing alarms.
gvAlarmEventType	IANAItuEventType Types of gvAlarmEventType: communicationsAlarm, qualityOfServiceAlarm, processingErrorAlarm, equipmentAlarm, environmentalAlarm.	.1.3.6.1.4.1.5584.2.3.3.1.4	The event type as described in IANA-ITU-ALARM-TC-MIB.

Attribute	Type	OID	Description
gvAlarmProbableCause	IANAItuProbableCause	.1.3.6.1.4.1.5584.2.3.3.1.5	The probable cause of the event as described in IANA-ITU-ALARM-TC-MIB.
gvAlarmComponentID	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.7	The string contains host name and fully distinguished name of sub-component under alarm. It maps to Event Code(s) and Instance Fields as name value pairs in the format – "TYPE=SBC, HOST=[host name], COMPONENT=[component name]. The TYPE and HOST strings are derived from the Ribbon Application Management Platform node attributes that are received during node registration. The Component string is derived as comma separated key value pairs; where the keys are Event Code(s)/Instance fields with the corresponding values received from the agent that generated the alarm.
gvAlarmAdditionalText	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.10	The Definition, Impact, Recommended Action, and Repetition as name value pairs.
alarmActiveDateAndTime	DateAndTime	.1.3.6.1.4.1.5584.2.3.3.1.2	The timestamp of the the event.
alarmActiveDescription	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.3	The description of the event.
gvAlarmEventTypeString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.12	The event type. If a device event type value is not found in IANA scheme and a custom text is included for for event type.
gvAlarmCauseString	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.11	The cause of the event. If device has not found a cause value in IANA scheme then this include a text value for cause.
gvAlarmName	SnmpAdminString	.1.3.6.1.4.1.5584.2.3.3.1.6	The original alarm name from the node.

Attribute	Type	OID	Description
gvAlarmManualClear	INTEGER	.1.3.6.1.4.1.5584.2.3.3.1.8	Specifies whether alarm clearing is manual or automatic. • 2 indicates automatic clearing. • 3 indicates manual clearing.

Number Portability Alarms

Contents

- [MNP Alarms](#)
 - [sonusEmsNPBulkFileReadyNotification](#)
 - [sonusEmsNPBulkFileRequestRejectedNotification](#)
 - [sonusEmsNPBulkProvisioningCompletedNotification](#)
 - [sonusEmsNPBulkProvisioningFailedNotification](#)
 - [sonusEmsLnpDataSyncErrorNotification](#)
- [LNP Adaptor Alarms](#)
 - [sonusEmsLnpBddFileDownloadErrorNotification](#)
 - [sonusEmsLnpBddFileDownloadCompletedNotification](#)
 - [sonusEmsLnpDataSyncErrorNotification \(LNP Adaptor\)](#)

This section covers alarms related to number portability services.

Ribbon Application Management Platform provides the following synchronization functionality to support number portability.

- Syniverse MNP
- Telcordia MNP
- LNP Adaptor

MNP Alarms

Contents

- [sonusEmsNPBulkFileReadyNotification](#)
- [sonusEmsNPBulkFileRequestRejectedNotification](#)
- [sonusEmsNPBulkProvisioningCompletedNotification](#)
- [sonusEmsNPBulkProvisioningFailedNotification](#)
- [sonusEmsLnpDataSyncErrorNotification](#)

This section covers alarms related to mobile number portability (MNP) services.

sonusEmsNPBulkFileReadyNotification**Type:** MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.85
Description	This alarm is raised by the Syniverse/Telcordia MNP listener service of the Ribbon Application Management Platform to indicate that the bulk file response is received for the request sent by the Ribbon Application Management Platform.
Repetition	No
Event Codes	sonusEmsNodeId —The internal ID of the node that was polled. sonusHostID —The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. SonusEventLevel — Provides event severity (critical, major, minor, informational), which is subsequently mapped to a Ribbon Application Management Platform display severity level. SonusEventClass — Lists the associated event class. SonusEventDescription — Describes the event. SonusEventTime — Provides timestamp of when the event occurs. sonusEmsNPServicesMCHName — Name of the vendor that hosts Mobile Number Portability Clearing House. sonusEmsNPServicesBulkRequestTransactionId — Transaction Id of the Bulk File Request sent to MCH.
Instance Fields	Node Name, Event Name, sonusEmsNPServicesMCHName, sonusEmsNPServicesBulkRequestTransactionId
Action	When the bulk file is generated, operator has to perform the following: 1. Logon to Syniverse/Telcordia MCH portal. 2. Download the file generated via HTTP/FTP to the local system. 3. In the Ribbon Application Management Platform, browse the file in the local system and perform Upload/Provision action, by selecting the request for which response is received.
Impact	MCH has generated the bulk file corresponding to request sent by the Ribbon Application Management Platform and is ready for download.
Clearing	Manual

sonusEmsNPBulkFileRequestRejectedNotification**Type:** WARNING

OID	1.3.6.1.4.1.2879.2.1.7.2.0.86
Description	This alarm is raised by the Syniverse/Telcordia MNP client of the Ribbon Application Management Platform, when the MCH rejects the Bulk file request sent.
Repetition	No
Event Codes	sonusEmsNodeId —The internal ID of the node that was polled. sonusHostId —The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. SonusEventLevel — Provides event severity (critical, major, minor, informational), which is subsequently mapped to a Ribbon Application Management Platform display severity level. SonusEventClass — Lists the associated event class. SonusEventDescription — Describes the event. SonusEventTime — Provides timestamp of when the event occurs. sonusEmsNPServicesMCHName — Name of the vendor that hosts Mobile Number Portability Clearing House. sonusEmsNPServicesBulkRequestTransactionId — Transaction Id of the Bulk File Request sent to MCH.
Instance Fields	Node Name, Event Name, sonusEmsNPServicesMCHName, sonusEmsNPServicesBulkRequestTransactionId
Action	Operator has to check the request sent and resend the bulk file request.
Impact	MCH has rejected the bulk file generation request. Possible reasons include incorrect time range, invalid user credentials.
Clearing	Manual

sonusEmsNPBulkProvisioningCompletedNotification

Type: WARNING

OID	1.3.6.1.4.1.2879.2.1.7.2.0.87
Description	This alarm is raised by the HostedLnpProvisioner of the Ribbon Application Management Platform when the provisioning of bulk file to PSX is completed successfully.

Repetition	No
Event Codes	sonusEmsNodeId —The internal ID of the node that was polled. sonusHostId —The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. SonusEventLevel — Provides event severity (critical, major, minor, informational), which is subsequently mapped to a Ribbon Application Management Platform display severity level. SonusEventClass — Lists the associated event class. SonusEventDescription — Describes the event. SonusEventTime — Provides timestamp of when the event occurs. sonusEmsNPServicesMCHName — Name of the vendor that hosts Mobile Number Portability Clearing House. sonusEmsNPServicesBulkRequestTransactionId — Transaction Id of the Bulk File Request sent to MCH.
Instance Fields	Node Name, Event Name, sonusEmsNPServicesMCHName, sonusEmsNPServicesBulkRequestTransactionId
Action	When the provisioning of all the bulk files (both full and partial are completed), the operator has to enable the MNP broadcast listener service to start real-time synchronization of MNP data.
Impact	Provisioning of Partial Bulk File to PSX is completed successfully.
Clearing	Manual

sonusEmsNPBulkProvisioningFailedNotification

Type: WARNING

OID	1.3.6.1.4.1.2879.2.1.7.2.0.88
Description	This alarm is raised by the HostedLnpProvisioner of the Ribbon Application Management Platform when the provisioning of bulk file to PSX is failed
Repetition	No

Event Codes	sonusEmsNodeId — The internal ID of the node that was polled. sonusHostId — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. SonusEventLevel — Provides event severity (critical, major, minor, informational), which is subsequently mapped to a Ribbon Application Management Platform display severity level. SonusEventClass — Lists the associated event class. SonusEventDescription — Describes the event. SonusEventTime — Provides timestamp of when the event occurs. sonusEmsNPServicesMCHName — Name of the vendor that hosts Mobile Number Portability Clearing House. sonusEmsNPServicesBulkRequestTransactionId — Transaction Id of the Bulk File Request sent to MCH.
Instance Fields	Node Name, Event Name, sonusEmsNPServicesMCHName, sonusEmsNPServicesBulkRequestTransactionId
Action	Operator has to identify the cause of failure from the mnp_trace_log, resolve the issue and re-provision the file.
Impact	Provisioning of Partial Bulk File is failed. Possible reasons include the following : 1. PSX pipe server is down. 2. POL-LNP-STORE license is not installed/associated to PSX. 3. Bulk file data is invalid. 4. Bulk file is not in a valid format. 5. No/Multiple PSX is registered in the Ribbon Application Management Platform.
Clearing	Manual

sonusEmsLnpDataSyncErrorNotification

This alarm is applicable to the MNP services.

Type: WARNING

OID	1.3.6.1.4.1.2879.2.1.7.2.0.84
Description	This alarm is raised by the Syniverse/Telcordia MNP listener service of the Ribbon Application Management Platform to indicate that the broadcast message sent by MCH is not provisioned to PSX.
Repetition	No

Event Codes	sonusEmsNodeId — The internal ID of the node that was polled. sonusHostId — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. SonusEventLevel — Provides event severity (critical, major, minor, informational), which is subsequently mapped to a Ribbon Application Management Platform display severity level. SonusEventClass — Lists the associated event class. SonusEventDescription — Describes the event. SonusEventTime — Provides timestamp of when the event occurs. sonusEmsNPServicesMCHName — Name of the vendor that hosts Mobile Number Portability Clearing House.
Instance Fields	Node Name, Event Name, sonusEmsNPServicesMCHName, sonusEmsNPServicesBulkRequestTransactionId
Action	Operator has to identify the cause of synchronization error from the mnp_trace_log and resolve the issue.
Impact	Real-time MNP data synchronization error. Possible reasons include the following: 1. MNP Listener service is not enabled. 2. Required license(EMS-LNP-FEED, POL-LNP-STORE) is not installed. 3. PSX pipe server is down. 4. No/Multiple PSX is registered in the Ribbon Application Management Platform.
Clearing	Manual

LNP Adaptor Alarms

Contents

- [sonusEmsLnpBddFileDownloadErrorNotification](#)
- [sonusEmsLnpBddFileDownloadCompletedNotification](#)
- [sonusEmsLnpDataSyncErrorNotification \(LNP Adaptor\)](#)

This section covers alarms related to local number portability (LNP). The LNP Adaptor synchronizes and sends LNP data received from the National Portability Administration Center (NPAC) SIP-IX to the Primary PSX. NPAC contains information for all ported and pooled numbers to support LNP in the US and Canada.

The LNP Adaptor alarm also includes sonusEmsLnpDataSyncErrorNotification, refer to [sonusEmsLnpDataSyncErrorNotification](#).

sonusEmsLnpBddFileDownloadErrorNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.82
Description	This alarm is raised by the BDDFileManager when it is unable to download the BDD files from the FTP server.
Repetition	No
Event Codes	sonusEmsNodeid—The internal ID of the node that was polled. sonusHostid—The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. SonusEventLevel — Provides event severity (critical, major, minor, informational), which is subsequently mapped to a Ribbon Application Management Platform display severity level. SonusEventClass — Lists the associated event class. SonusEventDescription— Describes the event. SonusEventTime—Provides timestamp of when the event occurs.
Instance Fields	sonusEmsNodeid.
Action	When there is a PARSE_ERROR, when you download the file, perform the following to obtain the last transaction ID: 1. Logon to the Ribbon Application Management Platform through telnet or ssh 2. Change the directory to <code><BASE_DIR>/weblogic/sonusEms/data/ lnp/tmp</code> 3. Extract the tar containing BDD files. 4. Move *SV*BDD and *BLOCK*BDD files to <code><BASE_DIR>/weblogic/sonusEms/data/lnp/final/</code> . These BDD file names contain last transaction ID The BDD file names for LNP data use the following format <code><Region>.<BDD_type>_BDD_PSTN_<DD-MM-YYYYHHMMSS>.<TRANS_ID></code> For example: <code>mw.lrn_BDD_PSTN_26-05-2009212322.1000074.bdd</code> The last transaction ID in the example is 1000074 and it is used for starting incremental changes 5. Use this transaction ID to start incremental changes by overriding last transaction ID.

Impact	Unable to download the BDD file.
Clearing	Manual.

sonusEmsLnpBddFileDownloadCompletedNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.83
Description	This alarm is raised by the BDDFile Manager when it correctly downloads the BDD file and is able to extract the last transaction ID.
Repetition	No.
Event Codes	sonusEmsNodeid—The internal ID of the node that was polled. sonusHostid—The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. SonusEventLevel — Provides event severity (critical, major, minor, informational), which is subsequently mapped to a Ribbon Application Management Platform display severity level. SonusEventClass — Lists the associated event class. SonusEventDescription— Describes the event. SonusEventTime—Provides timestamp of when the event occurs.
Instance Fields	sonusEmsNodeid
Action	None required.
Impact	Downloaded the BDD files successfully.
Clearing	Manual.

sonusEmsLnpDataSyncErrorNotification (LNP Adaptor)

This alarm is applicable to the LNP Adaptor.

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.84
Definition	This trap is raised by the SIP-IX Client on the Ribbon Application Management Platform to indicate the error while receiving the incremental changes.

Repetition	Yes.
Event Codes	sonusEmsNodeId—The internal ID of the node that was polled. sonusHostID—The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. SonusEventLevel — Provides event severity (critical, major, minor, informational), which is subsequently mapped to a Ribbon Application Management Platform display severity level. SonusEventClass — Lists the associated event class. SonusEventDescription— Describes the event. SonusEventTime—Provides timestamp of when the event occurs.
Instance Fields	sonusEmsNodeId
Action	Contact Ribbon Global Product Support (GPS) with your findings for the resolution.
Impact	Unable to fetch the error difference in the file download time.
Clearing	Manual

OSS Trap Resync Alarms

Contents

- [sonusEmsTrapReSyncDelimiterNotification](#)

This section covers alarms associated with the [OSS Trap Resync](#) process.

sonusEmsTrapReSyncDelimiterNotification

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.130

Description	Ribbon Application Management Platform (RAMP) sends a notification to the OSS when the trap resync starts or finishes.
Repetition	No
Event Codes	N/A
Instance Fields	sonusEventDescription, sonusEventLevel, sonusEmsFmTrapReSyncDelimiter The sonusEmsFmTrapReSyncDelimiter value is either 1 (start alarm) or 2 (stop alarm).
Action	None
Impact	None
Clearing	N/A

Performance Management Alarms

Contents

- [sonusEmsPMProfileAssignmentFailedNotification](#)
- [sonusEmsV2PMStatsFileCollectionFailed](#)
- [sonusEmsPMExportSFTPFailNotification](#)

This section covers alarms related to performance management.

sonusEmsPMProfileAssignmentFailedNotification

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.105
Description	This notification occurs when the PM profile assignment to the device fails even after the maximum retry attempts.
Repetition	Yes. Repeats each time the PM profile assignment fails to the device.

Event Codes	• sysName: An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. • sysObjectID: The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining `what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.' • sonusEventTime: Provides timestamp of when the event occurs. • sonusEventDescription: Describes the event. • sonusEventClass: Lists the associated event class. • sonusEventLevel: Lists the associated event level. • sonusEmsV2NodeIpAddressType: The address type of sonusEmsV2NodeIpAddress. • sonusEmsV2NodeIpAddress: The IP address of the node polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddress. • sonusEmsNodeid: The internal ID of the node that is polled.
Instance Fields	None
Action	Increase the read idle timeout for maximum retry attempts and try again. Wait for the command output to timeout.
Impact	The PM profile is not assigned to the device instance.
Clearing	Manual

sonusEmsV2PMStatsFileCollectionFailed

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.93
Description	The statistics download from the node fails.
Repetition	Yes. Repeats every time the PM collection task stops.

Event Codes	sysName: An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID: The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it assigns the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.' sonusEventTime: The timestamp of the event. sonusEventDescription: Description of the event. sonusEventClass: The associated event class. sonusEventLevel: The event severity (critical, major, minor, informational), which is subsequently mapped to a displayRAMP severity level. sonusEmsV2NodeIpAddressType: The address type of sonusEmsV2NodeIpAddress. sonusEmsV2NodeIpAddress: The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsNodeId: The internal ID of the node that was polled.
Instance Fields	sysName sysObjectID sonusEventTime sonusEventDescription sonusEventClass sonusEventLevel sonusEmsV2NodeIpAddressType sonusEmsV2NodeIpAddress sonusEmsNodeId
Action	Contact GPS.
Impact	Performance management statistics collection for the node fails.
Clearing	Manual

sonusEmsPMExportSFTPFailNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.1.31
Description	This alarm generates when the Ribbon Application Management Platform (RAMP) loses connectivity to the host IP and is no longer able to send statistics to the remote statistics server.
Repetition	This alarm repeats once for each remote server.
Event Codes	• sysName – Name of RAMP. • sonusEventTime – Time when the event occurred. • sonusEventDescription – Describes the event. • sonusEventClass - Lists the associated event class. • sonusEventLevel - Lists the associated event level (severity). • sonusRemoteServer – Remote server where SFTP fails.
Instance Fields	• sysName • sonusEventTime • sonusEventDescription • sonusEventClass • sonusEventLevel • sonusRemoteServer
Action	Check the accessibility of the remote server.
Impact	The export of the PM statistics fails on a remote location.
Clearing	Manual

RAMP CNF - Alarms

Note

There are no new RAMP CNF Alarms. The RAMP CNF supports all existing [RAMP Alarms](#).

Note

The [Resource Usage Threshold Crossing Alarms](#) are not supported for RAMP CNF.

Reachability Alarms

Contents

- [sonusEmsV2HostReachableNotification](#)
- [sonusEmsV2HostRestartedNotification](#)
- [sonusEmsV2HostUnreachableNotification](#)
- [sonusEmsV2NodeReachableNotification](#)
- [sonusEmsV2NodeRestartedNotification](#)
- [sonusEmsV2NodeUnreachableNotification](#)

This section covers alarms related to reachability management.

sonusEmsV2HostReachableNotification

This alarm is raised on the device, not on the Ribbon Application Management Platform (RAMP).

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.75
Description	The specified host is now reachable by RAMP.
Repetition	Yes. The Reachability Manager maintains the specified host's state. An alarm is generated each time the host's state transitions to 'reachable'.
Event Codes	sonusEmsNodeId—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	sonusEmsNodeId
Action	None required.

Impact	RAMP has established connectivity to the host.
Clearing	Automatic, clears in 2 minutes.

sonusEmsV2HostRestartedNotification

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.76
Description	The specified host has restarted since the last poll by the Ribbon Application Management Platform (RAMP).
Repetition	Yes. Repeats each time the sysUptime polled value is less than the last value.
Event Codes	sonusEmsNodeId—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	None.
Action	Investigate why the host restarted.
Impact	Any active sessions open to the host will terminate when the restart occurs. RAMP polls to the host during the restart period will fail.
Clearing	Manual.

sonusEmsV2HostUnreachableNotification

This alarm is raised on the device, not on the Ribbon Application Management Platform (RAMP).

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.74
Description	The HA physical interface is not reachable by RAMP.
Repetition	Yes. The Reachability Manager maintains the specified host's state. An alarm is generated each time the host's state transitions to 'unreachable'.
Event Codes	sonusEmsNodeId—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sonusEmsV2HostUnreachableNotification—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	sonusEmsNodeId
Action	Determine the reason connectivity is lost, and take action to rectify it. Possible reasons include, but are not limited to: • Network issues • Sonus agent not running on the host • Incorrect authentication information for host on RAMP
Impact	RAMP is unable to manage the node.
Clearing	Automatic, sonusEmsV2HostReachableNotification

sonusEmsV2NodeReachableNotification

This alarm is raised on the device, not on the Ribbon Application Management Platform (RAMP).

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.54
Description	The specified node is now reachable by RAMP. This alarm is also raised when the connection is restored between RAMP target and source nodes.
Repetition	Yes. The Reachability Manager maintains the specified node's state. An alarm is generated each time the node's state transitions to 'reachable'.
Event Codes	sonusEmsNodeid—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	sonusEmsNodeid
Action	None required.
Impact	None.
Clearing	Automatic, clears in 2 minutes.

sonusEmsV2NodeRestartedNotification

This alarm is raised on the device, not on the Ribbon Application Management Platform (RAMP).

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.55
Description	The specified node has restarted since last polled by RAMP.
Repetition	Yes. Repeats each time the sysUptime value of either host in an HA pair polled is less than the last value.
Event Codes	sonusEmsNodeId—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	sonusEmsNodeId
Action	No action required if restart is intentional. If not, investigate reason for node restart.
Impact	None.
Clearing	Manual.

sonusEmsV2NodeUnreachableNotification

This alarm is raised on the device, not on the Ribbon Application Management Platform (RAMP).

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.53

Description	Any type of registered device not reachable by RAMP. This alarm is also raised when target RAMP detects that it lost connection to source. The target RAMP sends the alarm to the configured OSS or NMS.
Repetition	Yes. The Reachability Manager maintains the specified node's state. An alarm is generated each time the node's state transitions to 'unreachable'.
Event Codes	sonusEmsNodeId—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	sonusEmsHostId
Action	Investigate loss of communication to the specified node. Verify the following: - Network connectivity to the device exists. - The maximum number of management clients has not been exceeded on the device. The GSX limits this to eight (8). Use the <code>CLI SHOW MGMT CLIENT SUMMARY</code> command to check this. - The following three settings are correct: - IP address - SNMP community strings To check the status of device, navigate to Device Management > Node Management > Function Manager.
Impact	Node cannot be managed by RAMP.
Clearing	Automatic, sonusEmsV2NodeReachableNotification

Redundancy Alarms

Contents

- [sonusHARACProcessDownNotification](#)
- [sonusHARACProcessUpNotification](#)
- [sonusHARACStateChangeNotification](#)
- [sonusHARACFailoverInitiatedNotification](#)
- [sonusHARACFailoverStandbyTimeoutNotification](#)
- [sonusHARACFailoverSuccessful](#)
- [sonusHARACFailoverFailed](#)
- [sonusHARACArbitratorDownNotification](#)
- [sonusHARACArbitratorUpNotification](#)

This section covers alarms related to Ribbon Application Management Platform (RAMP) redundancy.

sonusHARACProcessDownNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.5.3339.2.0.1
Description	A Ribbon Application Management Platform (RAMP) process is down.
Repetition	No, once a trap is sent another will not be sent unless it has been automatically cleared.

Event Codes	sonusHostID: The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusRACHostID: The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusRACProcess: Denotes the RAMP process which is down now. Processes are as follows: ◦ sonus.agent: Sonus Agent ◦ sonus.sbcManager: The SBC Manager ◦ sonus.callTraceListener: Call Trace Listener ◦ sonus.databaseCheck: Denotes the process to check whether the database is up and running on the host. ◦ sonus.dataHandler: PM Data Handler ◦ sonus.dask: PM Dask ◦ sonus.dbaaS: DBaaS (database) ◦ sonus.fileReplication: File Replication ◦ sonus.fmTrapReceiver: FM Trap Receiver ◦ sonus.ftp_pm: The PM FTP Poller. ◦ sonus.hotDeploy: Denotes the RAMP Jboss process after invoking Transition to Active MBean. ◦ sonus.idhService: IDH (optional feature). ◦ sonus.jmx_pm: PM JMX Poller. ◦ sonus.kafka: Kafka ◦ sonus.kafkaConnect: Kafka Connect. ◦ sonus.kafkaSchemaRegistry: Kafka Schema Registry. ◦ sonus.kafkaMirror: Kafka Mirroring. ◦ sonus.owl: The Owl. ◦ sonus.snmp_pm: The PM SNMP Poller. ◦ sonus.stiService: STI (optional feature). ◦ sonus.trapProbe: Trap Probe. ◦ sonus.warmDeploy: Denotes the process that Jboss is started in standby mode. ◦ sonus.apacheproxy: Denotes the process that ApacheProxy is started in active mode. ◦ sonus.zookeeper: The Zookeeper.
Instance Fields	sonusRACProcess sonusRACHostID
Action	Though OpenSAF tries to bring the process up and running again and the trap should be cleared, it would still be worth investigating why the process has gone down.
Impact	This may impact normal functioning of RAMP.
Clearing	Automatic, sonusHARACProcessUpNotification.

sonusHARACProcessUpNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.5.3339.2.0.2
Description	A Ribbon Application Management Platform (RAMP) process has successfully been started.
Repetition	No
Event Codes	sonusHostID: The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusRACHostID: Denotes unique host id in a RAC cluster. sonusRACProcess: Denotes the RAMP process which is up now. Processes are as follows: • sonus.agent: The Sonus Agent. • sonus.sbcManager: The SBC Manager • sonus.callTraceListener: Call Trace Listener. • sonus.databaseCheck: Denotes the process to check whether the database is up and running on the host. • sonus.dataHandler: PM Data Handler. • sonus.dask: The PM Dask. • sonus.dbaaS: DBaaS (database). • sonus.fileReplication: File Replication. • sonus.fmTrapReceiver: The FM Trap Receiver. • sonus.ftp_pm: The PM FTP Poller. • sonus.hotDeploy: Denotes the RAMP Jboss process after invoking Transition to Active MBean. • sonus.idhService: IDH (optional feature). • sonus.jmx_pm: PM JMX Poller. • sonus.kafka: Kafka • sonus.kafkaConnect: Kafka Connect. • sonus.kafkaSchemaRegistry: Kafka Schema Registry. • sonus.kafkaMirror: Kafka Mirroring. • sonus.owl: The Owl. • sonus.snmp_pm: The PM SNMP Poller. • sonus.stiService: STI (optional feature). • sonus.trapProbe: Trap Probe. • sonus.warmDeploy: Denotes the process that Jboss is started in standby mode. • sonus.apacheproxy: Denotes the process that ApacheProxy is started in active mode. • sonus.zookeeper: The Zookeeper.
Instance Fields	sonusRACProcess sonusRACHostID
Action	None
Impact	This may indicate that normal functioning of RAMP was impacted by the previous trap indicating that a process was down.

Clearing	Automatic

sonusHARACStateChangeNotification

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.5.3339.2.0.3
Description	This is a notification that the state of a Ribbon Application Management Platform (RAMP) node has been changed.
Repetition	No
Event Codes	sonusHARACPrevState: Denotes the previous state of this node. The previous high availability state of this node. • 0 offline • 1 active • 2 standby sonusHARACNewState: Denotes the new state of this node. The new high availability state of this node. • 0 offline • 1 active • 2 standby
Instance Fields	sonusHARACPrevState sonusHARACNewState
Action	Manual action can trigger a state change or automatic one. For the automatic state change the reason for state change trigger can be investigated.
Impact	This may impact normal functioning of RAMP.
Clearing	Manual

sonusHARACFailoverInitiatedNotification

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.5.3339.2.0.4
Description	This is to notify that a relocate action has been initiated to switch the roles of the system from active to standby and vice versa.
Repetition	No

Event Codes	sonusHARACFailoverReason: This describes the reason for the failure of the active box. sonusHARACClusterName: Denotes the name of the HA RAC Cluster.
Instance Fields	None
Action	None
Impact	The standby should become active.
Clearing	Manual

sonusHARACFailoverStandbyTimeoutNotification

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.5.3339.2.0.5
Description	This is to notify that, after failover, the original active node does not become standby within the set period of time.
Repetition	No
Event Codes	sonusHARACClusterName: Denotes the name of the HA RAC Cluster. sonusHARACNodeName: Denotes the name of the node.
Instance Fields	sonusHARACClusterName, sonusHARACNodeName
Action	Unless the node is intentionally brought down, or the failover does not succeed, check the log and other traps to check if any component failure prevents the node to become standby. It is also possible that the node takes longer time to recover and eventually becomes standby successfully, in that case this notification can be ignored.
Impact	After the original standby node takes over the active role, the original active node should normally become standby within 3 minutes after failover.
Clearing	Manual

sonusHARACFailoverSuccessful

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.5.3339.2.0.14

Description	This notifies that the switch over to the standby box has completed successfully.
Repetition	No
Event Codes	None
Instance Fields	None
Action	None
Impact	The standby becomes active.
Clearing	Manual

sonusHARACFailoverFailed

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.5.3339.2.0.15
Description	This notifies that the switch over to the standby box has failed.
Repetition	No
Event Codes	None
Instance Fields	None
Action	This needs to be investigated.
Impact	The standby could not become active.
Clearing	Manual

sonusHARACArbitratorDownNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.5.3339.2.0.16
Description	This is to notify that the etcd instance designated as the arbitrator is down. etcd is a leader-based distributed system.
Repetition	No

Event Codes	None
Instance Fields	sysName, sonusEventTime, sonusEventDescription, sonusEventLevel, sonusHARACArbitratorIp
Action	None
Impact	The auto-switchover does not work if the active RAMP node fails.
Clearing	Automatic, sonusHARACArbitratorUpNotification

sonusHARACArbitratorUpNotification

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.5.3339.2.0.17
Description	The etcd instance designated as the arbitrator is up.
Repetition	No
Event Codes	None
Instance Fields	sysName, sonusEventTime, sonusEventDescription, sonusEventLevel, sonusHARACArbitratorIp
Action	None
Impact	None
Clearing	Automatic

SBC Edge Alarms

Contents

- [ribbonDeviceNotConnectedLast24Hours](#)
- [ribbonDeviceNotConnectedLast24HoursClear](#)
- [ribbonDeviceNotConnectedLast90Days](#)
- [ribbonDeviceNotConnectedLast90DaysClear](#)
- [ribbonEVServiceZTPConnectivityLostClearNotification](#)

- [ribbonEVServiceZTPConnectivityLostNotification](#)
- [ribbonEVServiceZTPDeviceRetrievalFailedClearNotification](#)
- [ribbonEVServiceZTPDeviceRetrievalFailedNotification](#)
- [ribbonEVServiceZTPDeviceRetrievalFailedTimeBasedNotification](#)
- [ribbonEVServiceZTPNotRegisteredClearNotification](#)
- [ribbonEVServiceZTPNotRegisteredNotification](#)
- [ribbonEVServiceZTPRegisteredSucceededNotification](#)
- [ribbonEVServiceZTPRegistrationFailedNotification](#)
- [sbcEdgeHAInvalidC2eModeClearNotification](#)
- [sbcEdgeHAInvalidC2eModeNotification](#)
- [sbcEdgeHANodeCountInvalidClearNotification](#)
- [sbcEdgeHANodeCountInvalidNotification](#)
- [sbcEdgeHANodesDuplicateRoleClearNotification](#)
- [sbcEdgeHANodesDuplicateRoleNotification](#)
- [sbcEdgeHANodesSplitBrainClearNotification](#)
- [sbcEdgeHANodesSplitBrainNotification](#)
- [sbcEdgeHAStandbyNodeDownClearNotification](#)
- [sbcEdgeHAStandbyNodeDownNotification](#)

This section covers alarms related to managing SBC Edge devices.

ribbonDeviceNotConnectedLast24Hours

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.156
Description	The SBC Edge device has not checked in with Ribbon Application Management Platform (RAMP) for 24 hours.
Repetition	Yes, repeats every midnight until the SBC Edge device checks-in.
Event Codes	• sonusEventTime: The timestamp of the event. • sonusEventDescription: The description of the event. • sonusEventClass: The event class. • sonusEventLevel: The event level.
Instance Fields	sonusHostID : The unique ID or serial number for this host.
Action	Check the connectivity between the SBC Edge device and RAMP.
Impact	The SBC Edge device is unable to communicate with RAMP.
Clearing	Automatic, ribbonDeviceNotConnectedLast24HoursClear

ribbonDeviceNotConnectedLast24HoursClear

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.157
Description	The SBC Edge device has now checked in with Ribbon Application Management Platform (RAMP). The clear alarm for ribbonDeviceNotConnectedLast24Hours .
Repetition	No
Event Codes	- sonusEventTime: The timestamp of the event. - sonusEventDescription: The description of the event. - sonusEventClass: The event class. - sonusEventLevel: The event level.
Instance Fields	sonusHostID: The unique ID or serial number for this host.
Action	None
Impact	The SBC Edge device has resumed communication with RAMP.
Clearing	Automatic

ribbonDeviceNotConnectedLast90Days

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.158
Description	The SBC Edge device has not checked in with Ribbon Application Management Platform (RAMP) for the last 90 days.
Repetition	Yes, repeats every midnight until the SBC Edge device checks-in.
Event Codes	- sonusEventTime: The timestamp of the event. - sonusEventDescription: The description of the event. - sonusEventClass: The event class. - sonusEventLevel: The event level.
Instance Fields	sonusHostID: The unique ID or serial number for this host.
Action	Check the connectivity between the SBC Edge device and RAMP.
Impact	The SBC Edge device is unable to communicate with RAMP.
Clearing	Automatic, ribbonDeviceNotConnectedLast90DaysClear

ribbonDeviceNotConnectedLast90DaysClear

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.159
Description	The SBC Edge device has checked in with Ribbon Application Management Platform (RAMP). The clear alarm for ribbonDeviceNotConnectedLast90Days .
Repetition	No
Event Codes	• sonusEventTime: The timestamp of the event. • sonusEventDescription: The description of the event. • sonusEventClass: The event class. • sonusEventLevel: The event level.
Instance Fields	sonusHostID: The unique ID or serial number for this host.
Action	None
Impact	The SBC Edge device has resumed communication with RAMP.
Clearing	Automatic

ribbonEVServiceZTPConnectivityLostClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.152
Description	EdgeView service establishes connection with Zero Touch Provisioning (ZTP) server. The clear alarm for ribbonEVServiceZTPConnectivityLostNotification .
Repetition	No
Event Codes	• sonusHostID: The unique ID or serial number for this host. • sonusEventTime: The timestamp of the event. • sonusEventDescription: The description of the event. • sonusEventClass: The event class. • sonusEventLevel: The event level.
Instance Fields	None
Action	None

Impact	None
Clearing	Automatic

ribbonEVServiceZTPConnectivityLostNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.151
Description	The EdgeView service lost connectivity with the Zero Touch Provisioning (ZTP) server.
Repetition	Yes
Event Codes	- sonusHostID: The unique ID or serial number for this host. - sonusEventTime: The timestamp of the event. - sonusEventDescription: The description of the event. - sonusEventClass: The event class. - sonusEventLevel: The event level.
Instance Fields	None
Action	Check the connectivity between the EdgeView service and the ZTP server.
Impact	- If an SBC Edge node is trying register with Ribbon Application Management Platform (RAMP) for the first time, registration fails. - If an SBC Edge node is trying to re-register with RAMP, registration succeeds using the details in the RAMP database. - ZTP APIs will not work.
Clearing	Automatic, ribbonEVServiceZTPConnectivityLostClearNotification

ribbonEVServiceZTPDeviceRetrievalFailedClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.154

Description	The EdgeView service successfully retrieved the details of the SBC Edge device from the Zero Touch Provisioning (ZTP) server. The clear alarm for ribbonEVServiceZTPDeviceRetrievalFailedNotification .
Repetition	No
Event Codes	• sonusHostID: The unique ID or serial number for this host. • sonusEventTime: The timestamp of the event. • sonusEventDescription: The description of the event. • sonusEventClass: The event class. • sonusEventLevel: The event level.
Instance Fields	None
Action	None
Impact	The SBC Edge node is successfully registered on Ribbon Application Management Platform (RAMP).
Clearing	Automatic

ribbonEVServiceZTPDeviceRetrievalFailedNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.153
Description	EdgeView service fails to retrieve details of the SBC Edge device from Zero Touch Provisioning (ZTP) server. However, ZTP server is accessible.
Repetition	Yes. This alarm is repeated whenever the device tries to re-register and the c2e retrieval from ZTP fails.
Event Codes	• sonusHostID: The unique ID or serial number for this host. • sonusEventTime: The timestamp of the event. • sonusEventDescription: The description of the event. • sonusEventClass: The event class. • sonusEventLevel: The event level.
Instance Fields	None
Action	Check the connectivity between EdgeView service and ZTP server.

Impact	- If an SBC Edge node is trying register with RAMP for the first time, registration fails. - If an SBC Edge node is trying to re-register with RAMP, registration succeeds using the details in the RAMP database.
Clearing	Automatic, ribbonEVServiceZTPDeviceRetrievalFailedClearNotification

ribbonEVServiceZTPDeviceRetrievalFailedTimeBasedNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.155
Description	The EdgeView service failed to retrieve the details of the SBC Edge device from the Zero Touch Provisioning (ZTP) server within the default interval. However, the ZTP server is accessible.
Repetition	Yes. This alarm is repeated whenever the device tries to register again and the c2e retrieval from ZTP fails.
Event Codes	- sonusEventTime – Time when the event occurred. - sonusEventDescription – Describes the event. - sonusEventClass - Lists the associated event class. - sonusEventLevel - Lists the associated event level (severity). - sonusHostID—The unique ID or serial number for this host.
Instance Fields	None
Action	Check the connectivity between the EdgeView service and the ZTP server.
Impact	The SBC Edge node registration with Ribbon Application Management Platform (RAMP) failed.
Clearing	Manual

ribbonEVServiceZTPNotRegisteredClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.144

Description	EdgeView device is registered with Zero Touch Provisioning (ZTP) server. The clear alarm for ribbonEVServiceZTPNotRegisteredNotification .
Repetition	No
Event Codes	• sonusHostID: The unique ID or serial number for this host. • sonusEventTime: The timestamp of the event. • sonusEventDescription: The description of the event. • sonusEventClass: The event class. • sonusEventLevel: The event level.
Instance Fields	• ribbonEVServiceZTPIpAddressType: The IP address type of the ZTP server. • ribbonEVServiceZTPIpAddress: The IP address of the ZTP server.
Action	None
Impact	None
Clearing	Automatic

ribbonEVServiceZTPNotRegisteredNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.143
Description	EdgeView service is not registered with Zero Touch Provisioning (ZTP) server.
Repetition	Yes
Event Codes	• sonusEventTime – Time when the event occurred. • sonusEventDescription – Describes the event. • sonusEventClass - Lists the associated event class. • sonusEventLevel - Lists the associated event level (severity).
Instance Fields	• ribbonEVServiceZTPIpAddressType - The IP address type of the ZTP server. • ribbonEVServiceATPIpAddress - The IP address of the ZTP server.
Action	Use the EdgeView GUI to register EdgeView service with the ZTP server.

Impact	Unable to register the SBC Edge node with Ribbon Application Management Platform (RAMP).
Clearing	Automatic, ribbonEVServiceZTPNotRegisteredClearNotification

ribbonEVServiceZTPRegisteredSucceededNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.146
Description	EdgeView service is successfully registered with Zero Touch Provisioning (ZTP) server. The clear alarm for ribbonEVServiceZTPRegistrationFailedNotification .
Repetition	No
Event Codes	• sonusEventTime: The timestamp of the event. • sonusEventDescription: The description of the event. • sonusEventClass: The event class. • sonusEventLevel: The event level.
Instance Fields	• ribbonEVServiceZTPIpAddressType: The IP address type of the ZTP server. • ribbonEVServiceATPIpAddress: The IP address of the ZTP server.
Action	None
Impact	None
Clearing	Automatic

ribbonEVServiceZTPRegistrationFailedNotification

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.145
Description	EdgeView service failed to register with Zero Touch Provisioning (ZTP) server.
Repetition	Yes

Event Codes	- sonusEventTime – Time when the event occurred. - sonusEventDescription – Describes the event. - sonusEventClass - Lists the associated event class. - sonusEventLevel - Lists the associated event level (severity).
Instance Fields	- ribbonEVServiceZTPIpAddressType - The IP address type of the ZTP server. - ribbonEVServiceATPIpAddress - The IP address of the ZTP server.
Action	Try to connect ZTP server again. Contact Ribbon Global Support if needed.
Impact	ZTP server is not available, unable to register EdgeView service.
Clearing	Automatic, ribbonEVServiceZTPRegisteredSucceededNotification

sbcEdgeHAInvalidC2eModeClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.172
Description	This alarm is raised to clear sbcEdgeHAInvalidC2eModeNotification .
Repitition	No
Event Codes	sonusHostID sonusEventDescription sonusEventClass sonusEventLevel sonusEventTime
Instance Fields	None
Action	Only HA devices with same c2e mode can be registered with RAMP.
Impact	Registration for the devices with incorrect c2e mode are rejected.
Clearing	Automatic

sbcEdgeHAInvalidC2eModeNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.168
Description	This alarm is raised if the registration request of Edge HA nodes have different c2e mode values.
Repetition	No
Event Codes	sonusHostID sonusEventDescription sonusEventClass sonusEventLevel sonusEventTime
Instance Fields	None
Action	Only Edge HA devices with the same c2e mode must be registered with RAMP.
Impact	HA will not be registered for nodes having different c2e modes.
Clearing	Automatic. sbcEdgeHAInvalidC2eModeClearNotification

sbcEdgeHANodeCountInvalidClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.163
Description	This alarm is raised after the sbcEdgeHANodeCountInvalidNotification alarm is raised for clearing from the FM side.
Repetition	No
Event Codes	sonusHostID sonusEventDescription sonusEventClass sonusEventLevel sonusEventTime
Instance Fields	None

Action	Alarm details will be deleted from the database.
Impact	HA pair will have correct node count.
Clearing	Automatic

sbcEdgeHANodeCountInvalidNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.162
Description	If less than two nodes are registered on an Edge HA pair then this alarm is raised.
Repetition	No
Event Codes	sonusHostID sonusEventDescription sonusEventClass sonusEventLevel sonusEventTime
Instance Fields	None
Action	Register only two nodes to an Edge HA pair.
Impact	The Device Manager may not be able to display the HA pair details correctly.
Clearing	Automatic, sbcEdgeHANodeCountInvalidClearNotification

sbcEdgeHANodesDuplicateRoleClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.165
Description	This is the clearing alarm for sbcEdgeHANodesDuplicateRoleNotification that is raised during registration, if the role type for both nodes is same.
Repetition	No

Event Codes	sonusHostID sonusEventDescription sonusEventClass sonusEventLevel sonusEventTime
Instance Fields	None
Action	None
Impact	Clears the trap sbcEdgeHANodesDuplicateRoleNotification
Clearing	Automatic

sbcEdgeHANodesDuplicateRoleNotification

Type: MINOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.164
Description	Swelite registration requests for an HA pair are considered valid if both the nodes have distinct role type. If the role type for both nodes is same then the EVService raises an alarm after accepting the registration request. This alarm is cleared once the role type is corrected/updated only through registration.
Repetition	No
Event Codes	sonusHostID sonusEventDescription sonusEventClass sonusEventLevel sonusEventTime
Instance Fields	None
Action	The role for any node can be updated to be an appropriate distinct through a new registration request.
Impact	1. An HA pair consists of only two nodes. If any more nodes are registered with RAMP then it is an incorrect depiction of HA pair. 2. The Device Manager UI may not be able to correctly display the HA pair details.

Clearing	Automatic, sbcEdgeHANodesDuplicateRoleClearNotification

sbcEdgeHANodesSplitBrainClearNotification

Type: CLEAR

OID	1.3.6.1.4,1.2879.2.1.7.2.0.171
Description	This alarm is raised if the split brain condition is resolved.
Repetition	No
Event Codes	sonusHostID sonusEventDescription sonusEventClass sonusEventLevel sonusEventTime
Instance Fields	None
Action	None
Impact	None
Clearing	Automatic

sbcEdgeHANodesSplitBrainNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.170
Description	This alarm is raised if there is a possibility of split brain situation.
Repetition	No
Event Codes	sonusHostID sonusEventDescription sonusEventClass sonusEventLevel sonusEventTime
Instance Fields	None

Action	Correct the role on the Device side and trigger the registration request.
Impact	The Device Manager may not be able to display the HA pair details correctly.
Clearing	Automatic, sbcEdgeHANodesSplitBrainClearNotification

sbcEdgeHASTandbyNodeDownClearNotification

Type: CLEAR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.167
Description	This alarm is raised after the sbcEdgeHASTandbyNodeDownNotification alarm for clearing it from FM side.
Repetition	No
Event Codes	sonusHostID sonusEventDescription sonusEventClass sonusEventLevel sonusEventTime
Instance Fields	None
Action	Alarm details are deleted from the DB.
Impact	The HA pair will have distinct role of nodes.
Clearing	Automatic

sbcEdgeHASTandbyNodeDownNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.166
Description	This alarm will be raised if the standby node on the Swelite HA pair goes down/offline.
Repetition	No

Event Codes	sonusHostID sonusEventDescription sonusEventClass sonusEventLevel sonusEventTime
Instance Fields	None
Action	1. Restart the device and ensure heartbeat is sent to RAMP. 2. If device is up and sending heartbeat, RabbitMQ service needs to be checked if its running. If RMQ service is down all the nodes should be marked offline.
Impact	The availability in the HA pair is compromised.
Clearing	Automatic, sbcEdgeHAStandbyNodeDownClearNotification

Threshold Alarms

Contents

- [sonusEmsV2FallingEventNotification](#)
- [sonusEmsV2RisingEventNotification](#)

This section covers alarms related to configured performance thresholds.

sonusEmsV2FallingEventNotification

This alarm is raised on the device, not on the Ribbon Application Management Platform.

Type: User-defined

OID	1.3.6.1.4.1.2879.2.1.7.2.0.52

Description	A falling event notification informs that a given performance measure for which a previous rising event notification was generated has returned below a defined falling value for that threshold and should be cleared.
Repetition	No. 1. The state is maintained. Once the rising threshold is breached, a sample value below the falling threshold causes this alarm to be generated. 2. Also, when the PM threshold config is changed (Observability -> Performance Management -> Thresholding), the alarm is generated.
Event Codes	sonusEmsThresholdIdentifier—A key that uniquely identifies this threshold for managing duplicate alarms and clearing (matching the falling and rising notifications). sonusEmsV2ThresholdIpAddress—The IP address of the device on which the threshold was crossed. The type of this address is determined by the value of sonusEmsV2ThresholdIpAddressType. sonusEmsV2ThresholdIpAddressType—The address type of sonusEmsV2ThresholdIpAddress. sonusEmsThresholdLocationIndexes—The indexes of the location within the device at which the threshold was crossed; may be shelf, slot number, interface number, trunk group number, etc., depending on where the threshold event occurred. sonusEmsThresholdObjectId—The OID of the performance measure that was crossed. sonusEmsThresholdSampleValue—The actual value measured that denotes that the threshold was crossed (should be greater than or equal to the rising trigger value or less than or equal to the falling trigger value). sonusEmsThresholdTriggerValue—The threshold value that was crossed (the rising or falling value set for the threshold). sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectId—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	sonusEmsThresholdObjectId, sonusEmsThresholdIdentifier
Action	Determined by each location.
Impact	None.
Clearing	Automatic, clears in 2 minutes.

sonusEmsV2RisingEventNotification

This alarm is raised on Ribbon Application Management Platform (RAMP). However, the error condition is on the device. Identify the device using the IP address included in the alarm description.

Type: User-defined

OID	1.3.6.1.4.1.2879.2.1.7.2.0.51
Description	A rising event notification informs that a given performance measure has crossed a given threshold (it has risen above a defined rising threshold value).
Repetition	alarm is generated once. Additional samples above the threshold do not cause this alarm to repeat. This alarm resets once the falling threshold is met.

Event Codes	sonusEmsThresholdIdentifier—A key that uniquely identifies this threshold for managing duplicate alarms and clearing (matching the falling and rising notifications). sonusEmsThresholdIpAddress—The IP address of the device on which the threshold was crossed. The type of this address is determined by the value of sonusEmsV2ThresholdIpAddressType. sonusEmsThresholdIpAddressType—The address type of sonusEmsV2ThresholdIpAddress. sonusEmsThresholdLocationIndexes—The indexes of the location within the device at which the threshold was crossed; may be shelf, slot number, interface number, trunk group number, etc., depending on where the threshold event occurred. sonusEmsThresholdObjectId—The OID of the performance measure that was crossed. sonusEmsThresholdSampleValue—The actual value measured that denotes that the threshold was crossed (should be greater than or equal to the rising trigger value or less than or equal to the falling trigger value). sonusEmsThresholdTriggerValue—The threshold value that was crossed (the rising or falling value set for the threshold). sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	Determined by each location.
Action	sonusEmsThresholdObjectId, sonusEmsThresholdIdentifier
Impact	User-defined.
Clearing	Automatic, sonusEmsV2FallingEventNotification

Verification Manager Alarms

Contents

- [sonusV2VfyMgrNodeTypeFailNotification](#)
- [sonusV2VfyMgrNodeTypeSuccessNotification](#)

This section covers alarms related to the Verification Manager. The Verification Manager listens for agent restart traps, determines which registered node(s) relate to the traps, and runs a verification task to ensure that the Ribbon Application Management Platform (RAMP) model of the device is correct.

sonusV2VfyMgrNodeTypeFailNotification

This alarms is raised on the device not on Ribbon Application Management Platform (RAMP).

Type: CRITICAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.64
Description	The agent on the host identified by sonusHostID does not contain the instrumentation component needed to manage the registered node. The RAMP models HA nodes as a single entity, however, each participating host can send traps that relate explicitly to that host using the sonusHostID component as the identifier.
Repetition	Yes. The Verification Manager maintains the state. This alarm is generated if a transition occurs.

Event Codes	sonusEmsNodeID—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sonusHostID—The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router'.
Instance Fields	sonusEmsNodeID
Action	Investigate why the application-specific management blade is not running on the host.
Impact	RAMP is unable to fully manage the device.
Clearing	Automatic, sonusV2VfyMgrNodeTypeSuccessNotification

sonusV2VfyMgrNodeTypeSuccessNotification

This alarm is raised on the device not on Ribbon Application Management Platform (RAMP).

Type: INFORMATIONAL

OID	1.3.6.1.4.1.2879.2.1.7.2.0.65
Description	The agent on the host identified by sonusHostID contains the instrumentation component needed to manage the registered node. The RAMP models HA nodes as a single entity, however, each participating host can send traps that relate explicitly to that host using the sonusHostID component as the identifier.

Repetition	Yes. The Verification Manager maintains the state. This alarm is generated if a transition occurs.
Event Codes	sonusEmsNodeId—The internal ID of the node that was polled. sonusEmsV2NodeIpAddress—The IP address of the node that was polled. The type of this address is determined by the value of sonusEmsV2NodeIpAddressType. sonusEmsV2NodeIpAddressType—The address type of sonusEmsV2NodeIpAddress. sonusHostId—The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sysName—An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string. sysObjectID—The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining 'what kind of box' is being managed. For example, if vendor 'Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its 'Fred Router.'
Instance Fields	sonusEmsNodeId
Action	None required.
Impact	None.
Clearing	Automatic, clears in 2 minutes

linkUp

Type: Cleared

OID	1.3.6.1.6.3.1.1.5.4
Definition:	This notification is raised when the Secondary interface state Up.
Action:	None required.
Clearing:	Automatic, clears in 2 minutes
Repetition:	No

Instance Fields:	ifIndex: Physical address
Event Code(s):	• sysName: An administratively assigned name for this managed node. By convention, this is the node's fully qualified domain name. If the name is unknown, the value is the zero-length string. • sonusEventTime: Provides timestamp of when the event occurs. • sonusEventDescription: Describes the event. • Physical address: IP address of Secondary interface. • ifDescr: Provides the Secondary interface description. • ifIndex: The Secondary Interface Id (e.g., 2)

linkDown

Type: Critical

OID	1.3.6.1.6.3.1.1.5.3
Definition:	This notification is raised when the Secondary interface state Down.
Action:	None required.
Clearing:	Automatic, linkUp
Repetition:	No
Instance Fields:	ifIndex: Physical address
Action	Do the following: 1. Determine what circumstances caused the link to go down and rectify. 2. Bring the link back up.
Event Code(s):	• sysName: An administratively assigned name for this managed node. By convention, this is the node's fully qualified domain name. If the name is unknown, the value is the zero-length string. • sonusEventTime: Provides timestamp of when the event occurs. • sonusEventDescription: Describes the event. • Physical address: IP address of Secondary interface. • ifDescr: Provides the Secondary interface description . • ifIndex: The Secondary Interface Id (e.g., 2)

Cross-Platform Alarms

Contents

- [Agent Framework Alarms](#)
 - [Alarm Field Definition](#)
 - [Agent Framework Alarm Categories](#)
 - [Communicator Chassis Alarm](#)
 - [Communicator Process Management Alarms](#)
- [Host Monitoring Alarms](#)
 - [Application Monitoring Alarms](#)
 - [Disk Monitoring Alarms](#)
 - [Performance Management Backlog Alarms](#)
 - [Resource Usage Threshold Crossing Alarms](#)
- [Resource Usage Threshold Matrix](#)

This guide provides information on agent framework and host-monitoring alarms.

Agent Framework Alarms

Contents

- [Alarm Field Definition](#)
- [Agent Framework Alarm Categories](#)
- [Communicator Chassis Alarm](#)
 - [sonusCommChassisStartupNotification](#)
 - [sonusCommChassisTestNotification](#)
 - [sonusCommChassisCriticalTestNotification](#)
 - [sonusCommChassisMajorTestNotification](#)
 - [sonusCommChassisMinorTestNotification](#)
 - [sonusCommChassisWarnTestNotification](#)
 - [sonusCommChassisClearTestNotification](#)
- [Communicator Process Management Alarms](#)
 - [sonusCommProcMgmtGiveUpRestartNotification](#)
 - [sonusCommProcMgmtProcessRestartedNotification](#)
 - [sonusCommProcMgmtProcessRestartFailureNotification](#)

This section covers Agent Framework alarms originating from the Ribbon Communicator. The Communicator is a software “management chassis” that allows device instrumentation modules (blades) to be dynamically deployed.

Alarm Field Definition

In this guide, alarm notifications are defined by the fields: Severity, Definition, Impact, Action, Clearing, Repetition, Instance Field(s), and Event Code(s).

- **Severity** — Represents the severity level assigned by the device, and is displayed in bold green font directly underneath the alarm name. Possible severity levels are: Critical, Major, Minor, and Informational.
- **Definition** — Describes the purpose of the alarm.
- **Impact** — Describes the impact to the system when the indicated failure or fault occurs.

- **Action** — Details action to take by the operator to eliminate/prevent the failure condition. When appropriate, step-by-step procedures will be provided.
- **Clearing** — This field identifies how an alarm clears from the Fault Manager Event List. Alarm clearing is either automatic or manual.
- **Repetition** — Identifies if an alarm is repeated for each occurrence of a particular failure relating to the same managed object instance. When appropriate, repetition interval information is included in this field.
- **Instance Fields** — By default, all alarms are instanced by source host and trap type. For some alarms, an Instance ID field is included to uniquely identify the alarms. The Instance ID is created by appending values of the instance fields to the default instance information. In this guide, when instance fields exist for an alarm, the Instance Fields category in the alarm description is populated with one or more instance fields.
- **Event Code(s)** — Identifies detailed event information contained in the alarm (event levels and classes, threshold types, clearing strings, and so forth). This field may not always be included

Agent Framework Alarm Categories

Agent Framework alarms are classified into the following categories:

- [Communicator Chassis Alarm](#)
- [Communicator Process Management Alarms](#)

Communicator Chassis Alarm

Contents

- [sonusCommChassisStartupNotification](#)
- [sonusCommChassisTestNotification](#)
- [sonusCommChassisCriticalTestNotification](#)
- [sonusCommChassisMajorTestNotification](#)
- [sonusCommChassisMinorTestNotification](#)
- [sonusCommChassisWarnTestNotification](#)
- [sonusCommChassisClearTestNotification](#)

sonusCommChassisStartupNotification

Definition	The Sonus Communicator Chassis has started. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Informational
Impact	Device management is not possible until the agent has restarted.

Action	Unless this is a manual agent shutdown, investigate the reason for agent restart.
Clearing	Manual
Repetition	No
Instance Fields	None
Event Code(s)	sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters.

sonusCommChassisTestNotification

Definition	This notification is for test purposes. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap.
Severity	Informational
Impact	None
Action	None Required
Clearing	Manual
Repetition	Yes
Instance Fields	sonusEventDescription
Event Code(s)	sonusEventDescription — A description of the event that generated the trap sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters

sonusCommChassisCriticalTestNotification

Definition	Test trap for critical severity
Severity	Critical

Impact	None
Action	None; information only
Clearing	Manual
Repetition	No
Instance Fields	sonusEventTime,sonusEventDescription,sonusEventClass,sonusEventLevel, sonusHostID
Event Codes	sonusEventTime: The date and time of the event that generated the trap.
	sonusEventDescription: A description of the event that generated the trap.
	sonusEventClass: The category of the event that generated the trap.
	sonusEventLevel: The severity level of the event that generated the trap.
	sonusHostID: The unique id or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It can contain non-numeric characters.

sonusCommChassisMajorTestNotification

Definition	Test trap for major severity
Severity	Major
Impact	None
Action	None; information only
Clearing	Manual
Repetition	No
Instance Fields	sonusEventTime,sonusEventDescription,sonusEventClass,sonusEventLevel, sonusHostID

Event Codes	sonusEventTime: The date and time of the event that generated the trap.
	sonusEventDescription: A description of the event that generated the trap.
	sonusEventClass: The category of the event that generated the trap.
	sonusEventLevel: The severity level of the event that generated the trap.
	sonusHostID: The unique id or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters.

sonusCommChassisMinorTestNotification

Definition	Test trap for minor severity
Severity	Minor
Impact	None
Action	None; information only
Clearing	Manual
Repetition	No
Instance Fields	sonusEventTime,sonusEventDescription,sonusEventClass,sonusEventLevel, sonusHostID
Event Codes	sonusEventTime: The date and time of the event that generated the trap.
	sonusEventDescription: A description of the event that generated the trap.
	sonusEventClass: The category of the event that generated the trap.
	sonusEventLevel: The severity level of the event that generated the trap.

sonusHostID: The unique id or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters.

sonusCommChassisWarnTestNotification

Definition	Test trap for warning severity
Severity	Warning
Impact	None
Action	None; information only
Clearing	Manual
Repetition	No
Instance Fields	sonusEventTime,sonusEventDescription,sonusEventClass,sonusEventLevel, sonusHostID
Event Codes	sonusEventTime: The date and time of the event that generated the trap.
	sonusEventDescription: A description of the event that generated the trap.
	sonusEventClass: The category of the event that generated the trap.
	sonusEventLevel: The severity level of the event that generated the trap.
	sonusHostID: The unique id or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters.

sonusCommChassisClearTestNotification

Definition	Test trap for clearing severity
Impact	None
Severity	Clearing
Action	None; information only
Clearing	Manual
Repetition	No
Instance Fields	sonusEventTime,sonusEventDescription,sonusEventClass,sonusEventLevel, sonusHostID
Event Codes	sonusEventTime: The date and time of the event that generated the trap.
	sonusEventDescription: A description of the event that generated the trap.
	sonusEventClass: The category of the event that generated the trap.
	sonusEventLevel: The severity level of the event that generated the trap.
	sonusHostID: The unique id or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters.

Communicator Process Management Alarms

Contents

- [sonusCommProcMgmtGiveUpRestartNotification](#)
- [sonusCommProcMgmtProcessRestartedNotification](#)
- [sonusCommProcMgmtProcessRestartFailureNotification](#)

sonusCommProcMgmtGiveUpRestartNotification

Definition	Process Management has given up attempting to restart the specified process. This will occur after Process Management has failed to restart the process a specified number of times over a specified time interval. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Major
Impact	Varies depending upon the process that failed and customer priorities.
Action	Do the following: 1. Investigate restart failure. 2. Examine log files and look for associated traps. 3. Restart process using <code>./sonusEms start <processName> script</code>. Refer to figure Process Management Notification Flow for a general methodology flow diagram.
Clearing	Manual
Repetition	No
Instance Fields	None
Event Code(s)	sonusCommProcMgmtProcessName — This object defines the process name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters.

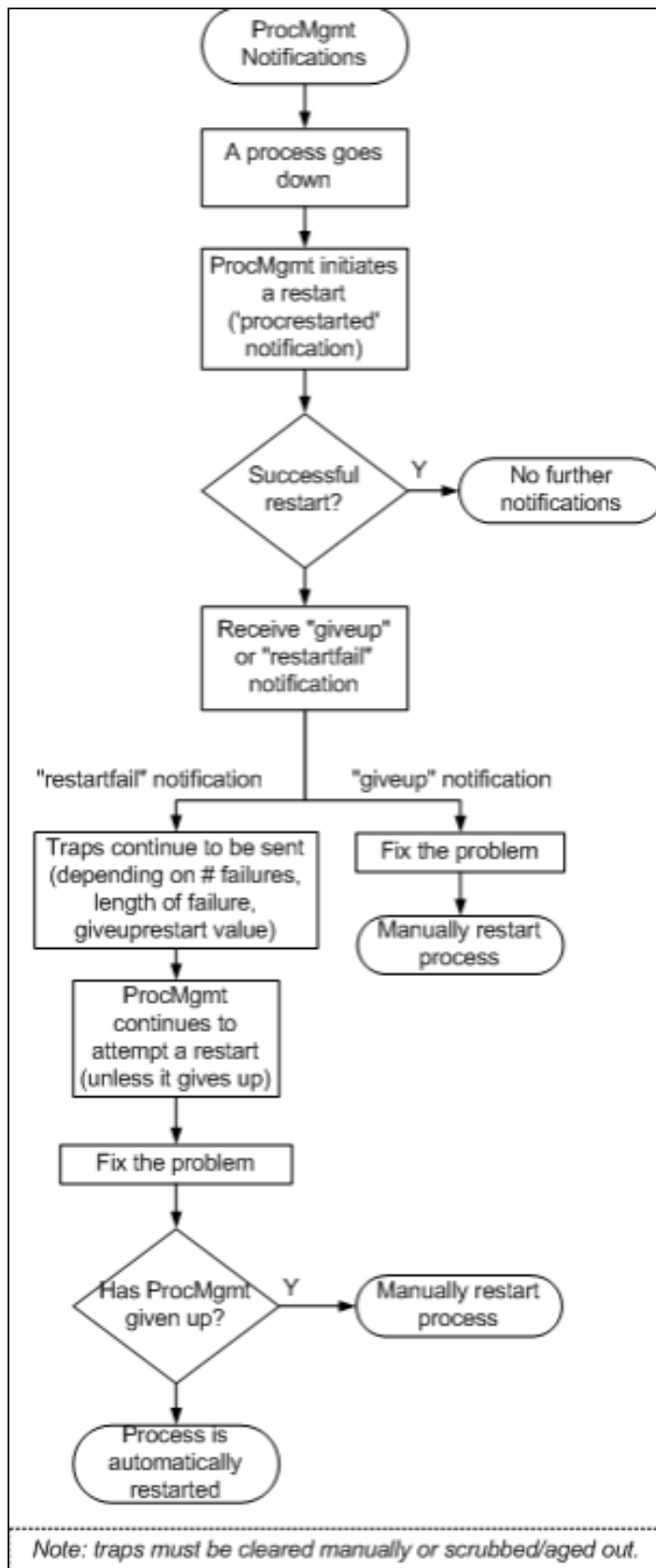
sonusCommProcMgmtProcessRestartedNotification

Definition	Process Management has given up attempting to restart the specified process. This will occur after Process Management has failed to restart the process a specified number of times over a specified time interval. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Major
Impact	Current service from the specified process may not be available.
Action	Do the following: 1. Investigate restart failure. 2. Examine log files and look for associated traps. 3. Look for associated traps. Once the problem is corrected, the process automatically restarts and returns to normal operation unless the restart process has timed out. If a restart time-out occurs, restart the process manually using <code>. / sonusEms start <processName> script.</code> Refer to figure Process Management Notification Flow for a general methodology flow diagram.
Clearing	Manual
Repetition	Yes. Depends on restart policy. If enabled and process continually fails, the alarm will be sent every restart interval until GiveUpRestart is sent.
Instance Fields	None
Event Code(s)	sonusCommProcMgmtProcessName — This object defines the process name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters.

sonusCommProcMgmtProcessRestartFailureNotification

Definition	An attempt by Process Management to restart the process specified by the object "sonusCommProcMgmtProcessName" has failed. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Major
Impact	The services provided by this process are not available.
Action	Do the following: 1. Investigate restart failure. 2. Examine log files and look for associated traps. 3. Look for associated traps. Once the problem is corrected, the process automatically restarts and returns to normal operation unless the restart process has timed out. If a restart time-out occurs, restart the process manually using <code>. / sonusEms start <processName> script</code>. Refer to figure Process Management Notification Flow for a general methodology flow diagram.
Clearing	Manual
Repetition	Yes. Depends on restart policy. If enabled and process continually fails, the alarm will be sent every restart interval until GiveUpRestart is sent.
Instance Fields	None
Event Code(s)	sonusCommProcMgmtProcessName — This object defines the process name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters.

Process Management Notification Flow



Host Monitoring Alarms

Contents

- [Application Monitoring Alarms](#)
 - [Process Number Mismatch](#)
 - [Process Termination](#)
- [Disk Monitoring Alarms](#)
 - [sonusHostDiskMonHardErrorNotification](#)
- [Performance Management Backlog Alarms](#)
 - [sonusEmsPMBacklogExportNotification](#)
 - [sonusHostPMStatsFileGenerationFailedNotification](#)
- [Resource Usage Threshold Crossing Alarms](#)
 - [CPU Usage Thresholds](#)
 - [Memory Usage Thresholds](#)
 - [Swap Space Usage Thresholds](#)
 - [File System Usage Thresholds](#)
 - [Application CPU Usage Thresholds](#)
 - [Application Memory Usage Thresholds](#)

This section covers the alarms generated and managed by the Host-Monitoring subagent.

Application Monitoring Alarms

Contents

- [Process Number Mismatch](#)
 - [sonusHostApplicationRuntimeErrorNotification](#)
 - [sonusHostApplicationRuntimeErrorRecoverNotification](#)
- [Process Termination](#)
 - [sonusHostApplicationExitNotification](#)
 - [sonusHostApplicationStartupNotification](#)

The host-monitoring agent monitors an application (see the table below for a list of applications per network element) by sending two sets of traps. For each application, it monitors the number of processes for this application plus the startup and exit of a process for this application.

Applications Per Network Element

PSX
ssmgr (PSX manager) ssa (PSX event generator)

Process Number Mismatch

Contents

- [sonusHostApplicationRuntimeErrorNotification](#)
- [sonusHostApplicationRuntimeErrorRecoverNotification](#)

When the number of processes do not match, the agent generates a problem alarm called *sonusHostApplicationRuntimeErrorNotification*. When the number of processes is matched, it generates *sonusHostApplicationRuntimeErrorRecoverNotification* alarm, which clears the previous problem alarm.

sonusHostApplicationRuntimeErrorNotification

Definition	Number of processes for an application do not match. This alarm is raised when license server process exits (shut down gracefully or forcefully) abnormally or normally. One alarm is raised for every license server. Run-time errors for application lserv occurs; mismatch in the number of expected instances and number of discovered instances.
Severity	Critical
Impact	One or more instance of a critical application on a host platform is not running. The impact is specific to the host platform. For example, on an SGX2000 platform, an eventProbe application is a critical application monitored by the agent. If no instance of eventProbe is running, the SGX2000 agent will generate this trap. The significance here is that the EMS and other management clients will lose alarms-monitoring capability to this particular SGX2000. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Action	Investigate immediately the events surrounding this alarm condition, and take appropriate action. The cause is most likely a major failure on the host platform.
Clearing	Automatic, sonusHostApplicationRuntimeErrorRecoverNotification
Repetition	No
Instance Fields	sonusHostExecName

Event Code(s)	sonusHostExpectedInstanceCount — Expected number of application instances. sonusHostExecName — The executable name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostSampleInstanceCount — Actual number of application instance from sampling poll.

sonusHostApplicationRuntimeErrorRecoverNotification

Definition	Number of processes for an application match. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters. Run-time errors for application lserv is recovered; the number of expected instances and number of discovered instances are same.
Severity	Clear
Impact	None
Action	None Required
Clearing	Automatic, clears in 2 minutes
Repetition	No
Instance Fields	sonusHostExecName
Event Code(s)	sonusHostExpectedInstanceCount — Expected number of application instances. sonusHostExecName — The executable name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostSampleInstanceCount — Actual number of application instance from sampling poll.

Process Termination

Contents

- [sonusHostApplicationExitNotification](#)
- [sonusHostApplicationStartupNotification](#)

Independently, if a process for the application exits, the agent generates the alarm [sonusHostApplicationExitNotification](#).

When a process for the application starts up, it generates the alarm [sonusHostApplicationStartupNotification](#).

The severity of these alarms is always Warning.

sonusHostApplicationExitNotification

Definition	A process for an application (see Table Application Per Network Element) exits. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters. This alarm is raised when license server process exits (shut down gracefully or forcefully). One alarm is raised for every license server.
Severity	Minor
Impact	The impact is specific to the host platform and the application running on it.
Action	Do the following: 1. Analyze events leading up to the exit of the application process for a root cause. 2. Determine whether this is a scheduled or unexpected event. 3. If this notification is unexpected, report the alarm to Ribbon Global Product Support (GPS) and troubleshoot further.
Clearing	Automatic, sonusHostApplicationStartupNotification
Repetition	Yes
Instance Fields	sonusHostExecName
Event Code(s)	sonusHostExecName — The executable name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostProcessID — The process ID

sonusHostApplicationStartupNotification

Definition	A process for an application (see Table Application Per Network Element) exits. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters. The alarm is raised when license server starts up.
Severity	Clear
Impact	None.
Action	None Required
Clearing	Automatic, clears in 2 minutes.
Repetition	No
Instance Fields	sonusHostExecName
Event Code(s)	sonusHostExecName — The executable name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostProcessID — The process ID

Disk Monitoring Alarms

This section lists the disk monitoring alarms on the Ribbon Application Management Platform (RAMP).

- [sonusHostDiskMonHardErrorNotification](#)

sonusHostDiskMonHardErrorNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.12.2.0.20

Description	This alarm triggers when a disk I/O error occurs. The RAMP uses a cron job to monitor the <code>/var/log/messages</code> file for any disk I/O errors every 30 minutes.
Repetition	No
Event Codes	sonusHostDiskDevName—Disk device name in descriptive format. sonusHostDiskErrorCount—Error count representing the difference between the last and present polled value. sonusHostID—The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters.
Instance Fields	sonusHostDiskDevName, sonusHostID.
Action	Perform the following to investigate the cause of the error: 1. Check the <code>/var/log/messages</code> logs for disk-related error messages. 2. Take note of potential impacts to the system as a result of the errors and contact Ribbon Global Product Support if normal operations are affected.
Impact	The impact depends on the disk reporting the errors. Frequent disk errors may indicate imminent failure. Determine which file system is affected by a failure using: <pre>df -hk</pre>
Clearing	Manual

Performance Management Backlog Alarms

Contents

- [sonusEmsPMBacklogExportNotification](#)
- [sonusHostPMStatsFileGenerationFailedNotification](#)

This section covers alarms generated for performance management backlog.

sonusEmsPMBacklogExportNotification

Type: MAJOR

OID	1.3.6.1.4.1.2879.2.1.7.2.0.110

Definition	This notification indicates the occurrence of a Ribbon Application Management Platform (RAMP) export of a performance management backlog file for a node.
Impact	RAMP backlog files are collected for the specified node.
Action	No action required.
Clearing	Manual
Repetition	This alarm is triggered when backlog is collected.
Instance Fields	
Event Code(s)	• sysName • sysObjectID • sonusEventTime • sonusEventDescription • sonusEventClass • sonusEventLevel • sonusEmsV2NodeIpAddressType • sonusEmsV2NodeIpAddress • sonusEmsNodeid

sonusHostPMStatsFileGenerationFailedNotification

Definition	Reports an event when the generation of a Performance Statistics tar file fails. Detailed message are specified in <i>sonusEventDescription</i>.
Severity	Major
Impact	PM SFTP will fail to collect .tar files for that specific interval.
Action	Check the agent logs.
Clearing	
Repetition	Whenever file creation fails in PSX agent, this alarm will be triggered.
Instance Fields	
Event Code(s)	INFO

Resource Usage Threshold Crossing Alarms

Contents

- CPU Usage Thresholds
 - [sonusHostCpuAvgUsageFallingThresholdNotification](#)
 - [sonusHostCpuAvgUsageRisingThresholdNotification](#)
 - [sonusHostCpuUsageFallingThresholdNotification](#)
 - [sonusHostCpuUsageRisingThresholdNotification](#)
- Memory Usage Thresholds
 - [sonusHostMemUsageFallingThreshldNotification](#)
 - [sonusHostMemUsageRisingThreshldNotification](#)
- Swap Space Usage Thresholds
 - [sonusHostSwapUsageFallingThresholdNotification](#)
 - [sonusHostSwapUsageRisingThresholdNotification](#)
- File System Usage Thresholds
 - [sonusHostFsUsageFallingThresholdNotification](#)
 - [sonusHostFsUsageRisingThresholdNotification](#)
- Application CPU Usage Thresholds
 - [sonusHostApplCpuUsageFallingThresholdNotification](#)
 - [sonusHostApplCpuUsageRisingThresholdNotification](#)
- Application Memory Usage Thresholds
 - [sonusHostApplMemUsageFallingThresholdNotification](#)
 - [sonusHostApplMemUsageRisingThresholdNotification](#)

Note

Refer to [Resource Usage Threshold Matrix](#) for a listing of threshold values for each severity level per network element as they relate to the following alarm categories.

Sample values used for the thresholding calculations are available in the following files on the host that originated alarm in the agent logs directory:

- resources.stats.audit
- application.stats.audit

CPU Usage Thresholds

Contents

- [sonusHostCpuAvgUsageFallingThresholdNotification](#)
- [sonusHostCpuAvgUsageRisingThresholdNotification](#)
- [sonusHostCpuUsageFallingThresholdNotification](#)
- [sonusHostCpuUsageRisingThresholdNotification](#)

sonusHostCpuAvgUsageFallingThresholdNotification

Definition	This “clear” alarm is generated when the CPU average usage (among all CPUs) falls below the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Critical/Minor/Major
Impact	None
Action	None required
Clearing	Automatic, clears in 2 minutes
Repetition	No
Instance Fields	sonusHostThresholdName
Event Code(s)	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value.

sonusHostCpuAvgUsageRisingThresholdNotification

Definition	This alarm is generated when the CPU average usage (among all CPUs) rises above the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Critical/Major/Minor

Impact	CPU processing may be degraded.
Action	Do the following: 1. Check application log files to monitor for failures. 2. To find out the CPU usage, run the following commands: ◦ <code>vmstat</code> — To find an initial view of the overall CPU usage behavior ◦ <code>sar -q</code> — To find the length of the run queue ◦ <code>uptime</code> — To find the recent load averages ◦ <code>mpstat</code> — To identify the consumption per cpu averages This helps you to isolate whether the cpu usage utilizes too much work (run queue and load averages) or resource constraint (cpu:sy) or process (cpu:us), and identifies the processes that utilizes the maximum cpu (<code>prstat -cLm</code>) 3. Contact Ribbon Global Product Support (GPS) for assistance
Clearing	Automatic, <code>sonusHostCpuAvgUsageFallingThresholdNotification</code>
Repetition	No
Instance Fields	<code>sonusHostThresholdName</code>
Event Code(s)	<code>sonusHostClrSet</code> — Alarm clear and set flag for an event. <code>sonusHostCpuID</code> — CPU identifier. <code>sonusHostID</code> — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. <code>sonusHostThresholdName</code> — Threshold name configured for a threshold-crossing notification. <code>sonusHostThresholdSampleValue</code> — Actual sampling value that trigger a threshold-crossing event. <code>sonusHostThresholdTriggerValue</code> — Threshold trigger value.

sonusHostCpuUsageFallingThresholdNotification

Definition	This alarm is generated whenever an individual CPU usage falls below the established threshold. The <code>sonusHostID</code> component of this trap specifies a unique identifier of the particular host that sent the trap. <code>sonusHostID</code> object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.

Severity	Informational
Impact	None
Action	None required
Clearing	Automatic, clears in 2 minutes
Repetition	No
Instance Fields	sonusHostThresholdName
Event Code(s)	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostCpuID — CPU identifier. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value.

sonusHostCpuUsageRisingThresholdNotification

Definition	This alarm is generated whenever an individual CPU usage rises above the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters
Severity	User-defined
Impact	CPU usage on the host exceeds what users are expecting.
Action	Check to see if any application is using too much CPU time, or if the processor speed is adequate for your environment and configuration.
Clearing	Automatic, sonusHostCpuUsageFallingThresholdNotification

Repetition	No
Instance Fields	sonusHostThresholdName
Event Code(s)	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostCpuID — CPU identifier. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value.

Memory Usage Thresholds

Contents

- [sonusHostMemUsageFallingThrshldNotification](#)
- [sonusHostMemUsageRisingThrshldNotification](#)

Note
See the [Resource Usage Threshold Matrix](#) for a breakdown of threshold values per severity level.

Sample values used for the thresholding calculations are available in these files on the host that originated the alarm in the agent logs directory:

- resources.stats.audit
- application.stats.audit

sonusHostMemUsageFallingThrshldNotification

OID	1.3.6.1.4.1.2879.2.1.12.2.0.8

Definition	This “clear” alarm is generated whenever the memory usage falls below the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Critical/Major/Minor
Impact	None
Action	None required
Clearing	Automatic, clears in 2 minutes
Repetition	No
Instance Fields	sonusHostThresholdName
Event Code(s)	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value.

sonusHostMemUsageRisingThrshldNotification

OID	1.3.6.1.4.1.2879.2.1.12.2.0.9
Definition	This alarm is generated whenever the memory usage rises above the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters

Severity	Critical/Major/Minor
Impact	If memory runs out, applications may slow down, cease to function, or crash.
Action	Do the following: 1. Check application log files to monitor if any failures arise. 2. Run the “top” utility to determine which process is using a large amount of the system resource. 3. Contact Ribbon Global Product Support (GPS) for assistance.
Clearing	Automatic, sonusHostMemUsageFallingThrshldNotification
Repetition	No
Instance Fields	sonusHostThresholdName
Event Code(s)	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value.

Swap Space Usage Thresholds

Contents

- [sonusHostSwapUsageFallingThresholdNotification](#)
- [sonusHostSwapUsageRisingThresholdNotification](#)

Note

See the [Resource Usage Threshold Matrix](#) for a breakdown of threshold values per severity level.

Sample values used for the thresholding calculations are available in these files on the host that originated the alarm in the agent logs directory:

- resources.stats.audit
- application.stats.audit

sonusHostSwapUsageFallingThresholdNotification

Definition	This “clear” alarm is generated whenever the swap space usage falls below the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Critical/Major/Minor
Impact	none
Action	None required
Clearing	Automatic, clears in two minutes
Repetition	No
Objects	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value.

sonusHostSwapUsageRisingThresholdNotification

Definition	This alarm is generated when swap space usage rises above the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.

Severity	Warning
Impact	No impact on the applications.
Action	None
Clearing	Automatic, sonusHostSwapUsageFallingThresholdNotification
Repetition	No
Objects	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value.

File System Usage Thresholds

Contents

- [sonusHostFsUsageFallingThresholdNotification](#)
- [sonusHostFsUsageRisingThresholdNotification](#)

Note

See the [Resource Usage Threshold Matrix](#) for a breakdown of threshold values per severity level.

Also note that the following file system types are not monitored:

- proc — Special file system for process table
- fd — Fixed disk (floppy, CD-ROM, etc.)
- autofs — auto-mounted file systems
- hsfs — High Sierra file system

Sample values used for the thresholding calculations are available in these files on the host that originated alarm in the agent logs directory:

- resources.stats.audit
- application.stats.audit

sonusHostFsUsageFallingThresholdNotification

Definition	This “clear” alarm is generated when file system usage falls below the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Critical/Major/Minor
Impact	None
Action	None Required
Clearing	Automatic, clears in 2 minutes
Repetition	No
Instance Fields	sonusHostThresholdName
Event Code(s)	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostFileSystemPath — File system path name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value.

sonusHostFsUsageRisingThresholdNotification

Definition	This alarm is generated when file system usage rises above the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Critical/Informational
Impact	If file system runs out, applications may slow down, cease to function, or even crash.
Action	Do the following: Check application log files to monitor if any failures arise. Use the <code>du</code> and <code>df</code> utilities to determine file system usage. Contact Ribbon Global Product Support for assistance.
Clearing	Automatic, sonusHostFsUsageFallingThresholdNotification
Repetition	No
Instance Fields	sonusHostThresholdName
Event Code(s)	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostFileSystemPath — File system path name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value

Application CPU Usage Thresholds

Contents

- [sonusHostApplCpuUsageFallingThresholdNotification](#)

- [sonusHostApplCpuUsageRisingThresholdNotification](#)

Note

See the [Resource Usage Threshold Matrix](#) for a breakdown of threshold values per severity level.

Sample values used for the thresholding calculations are available in these files on the host that originated the alarm in the agent logs directory:

- resources.stats.audit
- application.stats.audit

sonusHostApplCpuUsageFallingThresholdNotification

Definition	This “clear” alarm is generated when the host application CPU usage falls below the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Major/Informational
Impact	None
Action	None required
Clearing	Automatic, clears in 2 minutes
Repetition	No
Instance Fields	sonusHostThresholdName

Event Code(s)	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostExecName — The executable name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostProcessID — The process identifier. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value.

sonusHostApplCpuUsageRisingThresholdNotification

Definition	This alarm is generated when the host application CPU usage rises above the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Major/Informational
Impact	If the host application CPU usage runs out, applications may slow down, cease to function, or crash.
Action	Do the following: 1. Check application log files to monitor if any failures arise. 2. Run the “top” utility to determine which process is using a large amount of the system resource. 3. Contact Ribbon Global Product Support for assistance.
Clearing	Automatic, sonusHostApplCpuUsageFallingThreshold
Repetition	No
Instance Fields	sonusHostThresholdName

Event Code(s)	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostExecName — The executable name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostProcessID — The process identifier. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value.

Application Memory Usage Thresholds

Contents

- [sonusHostApplMemUsageFallingThresholdNotification](#)
- [sonusHostApplMemUsageRisingThresholdNotification](#)

Note

See the [Resource Usage Threshold Matrix](#) for a breakdown of threshold values per severity level.

Sample values used for the thresholding calculations are available in these files on the host that originated the alarm in the agent logs directory:

- resources.stats.audit
- application.stats.audit

sonusHostApplMemUsageFallingThresholdNotification

Definition	This “clear” alarm is generated when the host application memory usage falls below the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.

Severity	Major/Informational
Impact	None
Action	None required
Clearing	Automatic, clears in 2 minutes
Repetition	No
Instance Fields	sonusHostThresholdName
Event Code(s)	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostExecName — The executable name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostProcessID — The process identifier. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value.

sonusHostApplMemUsageRisingThresholdNotification

Definition	This alarm is generated when the host application memory usage rises above the established threshold. The sonusHostID component of this trap specifies a unique identifier of the particular host that sent the trap. sonusHostID object: The unique ID or serial number for the specified host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine, and may contain non-numeric characters.
Severity	Major/Informational
Impact	If the host application memory usage runs out, applications may slow down, cease to function, or crash.

Action	Do the following: Check application log files to monitor if any failures arise. Run the “top” utility to determine which process is using a large amount of the system resource. Contact Ribbon Global Product Support for assistance.
Clearing	Automatic, sonusHostApplMemUsageFallingThresholdNotification
Repetition	No
Instance Fields	sonusHostThresholdName
Event Code(s)	sonusHostClrSet — Alarm clear and set flag for an event. sonusHostExecName — The executable name. sonusHostID — The unique ID or serial number for this host. The serial number is an ASCII representation of the hardware-specific serial number of the physical machine. It may contain non-numeric characters. sonusHostProcessID — The process identifier. sonusHostThresholdName — Threshold name configured for a threshold-crossing notification. sonusHostThresholdSampleValue — Actual sampling value that trigger a threshold-crossing event. sonusHostThresholdTriggerValue — Threshold trigger value

Resource Usage Threshold Matrix

The thresholds for raising the threshold alarms on Ribbon Application Management Platform (RAMP) are listed in this section.

Resource Usage Threshold Matrix:

Threshold Type: associated alarms	DSI	RAMP	PSX
CPU Usage Thresholds: sonusHostCpuUsageRisingThresholdNotification sonusHostCpuUsageFallingThresholdNotification sonusHostCpuAvgUsageRisingThresholdNotification sonusHostCpuAvgUsageFallingThresholdNotification	Minor: 50% - 45% Major: 70% - 65% Critical: 90% - 85%	Minor: 50% - 45% Critical: 90% - 85%	Minor: 70%-65% Major: 80%-75% Critical: 90%-85%
Memory Usage Thresholds: sonusHostMemUsageRisingThresholdNotification sonusHostMemUsageFallingThresholdNotification	Minor: 85%-80% Major: 95%-90%	Minor: 85%-80% Major: 95%-90%	Major: 95%-90%
Swap Space Usage sonusHostSwapUsageRisingThresholdNotification sonusHostSwapUsageFallingThresholdNotification	Minor: 85%-80% Critical: 95%-90%	Minor: 85%-80% Critical: 95%-90%	Critical: 95%-90%
File System Usage: sonusHostFsUsageRisingThresholdNotification sonusHostFsUsageFallingThresholdNotification	Warning: 85% - 80% Critical: 95% - 90%	Warning: 85% - 80% Critical: 95% - 90%	Critical: 95% - 85%
Application CPU Usages Thresholds: sonusHostApplCpuUsageRisingThresholdNotification sonusHostApplCpuUsageFallingThresholdNotification	Java ¹ pltfm_probes³ Major: 50%-48% Warning: 20%-18%	Java ² Major: 50%-48% Warning: 20%-18% pltfm_probes³ Major: 50%-48% Warning: 20%-18%	Java ¹ Major: 50%-48% Warning: 20%-18% pltfm_probes³ Major: 50%-48% Warning: 20%-18% pipe & children processes Major: 40%-35% dbrepd and children processes Major: 40%-35%

Threshold Type: associated alarms	DSI	RAMP	PSX
Application Memory Usages Thresholds: sonusHostApplMemUsageRisingThresholdNotification sonusHostApplMemUsageFallingThresholdNotification	Java ¹ pltfrm_probes³ Major: 50%-48% Warning: 20%-18%	Java ² Major: 50%-48% Warning: 20%-18% pltfrm_probes³ Major: 50%-48% Warning: 20%-18%	Java ¹ Major: 50%-48% Warning: 20%-18% pltfrm_probes³ Major: 50%-48% Warning: 20%-18% pipe & children processes Major: 40%-35% dbrepd and children processes Major: 40%-35%

¹ Agent process

² All Java processes

³ Host/platform monitoring probes

Fault Management

In this section:

- [Planning for Fault Management](#)
- [Enable Sending Alarms from Devices to RAMP](#)
- [Customize the Alarm Interface](#)
- [Work with Active Alarms on the FM Dashboard](#)
- [View Alarm History](#)
- [Reclassify the Alarm Content](#)
- [Send Email Notifications](#)
- [Send Alarms to an External Destination](#)
- [Administer Fault Management](#)

Related articles:

- [Fault Management Workflows](#)
- [Work with Active Alarms](#)
- [Work with Alarm History](#)
- [Purge Alarms](#)
- [Reclassify Alarm Content](#)
- [Send Email Notifications for Alarms](#)
- [Forward Alarms to an External Destination](#)
- [Monitor Fault Management Activity](#)

The goal of fault management is to quickly identify device and network conditions that require attention so that a business can take action before negative consequences result. The Ribbon Application Management Platform (RAMP) Fault Management (FM) service is a common collection point for alarms coming from all of the managed devices registered with RAMP. RAMP provides a highly-customizable interface for working with these alarms in real-time and also supports sending alarms to an external system using the SNMP protocol.

The following sections introduce the key concepts and capabilities of RAMP fault management.

Planning for Fault Management

Each enterprise must determine the most effective strategy for managing the flow of alarms coming from their network devices. The FM user interface provides a wide range of controls that determine which alarms are presented to a user. For example, you might configure the system so that particular users see alarms from devices of a particular type, or from devices in a particular region, or alarms that are categorized with a critical severity.

To enable this type of flexibility, RAMP administrators must coordinate their FM configuration with their use of resource groups and user groups. Resource groups logically group devices within the network and user groups determine which users can work with particular resource groups. Therefore, administrators must be sure that devices whose alarms should be viewed together are part of the same resource group. Similarly, they must ensure that users who will work with those alarms are members of user groups that have access to the resource group.

Refer to [Work with Resource Groups](#) for more information on resource groups.

Refer to [Add User Groups](#) for more information on user groups.

Enable Sending Alarms from Devices to RAMP

Once a device is registered with RAMP, either manually or dynamically, alarms generated by the device are sent to RAMP. No additional configuration is required to enable sending faults to RAMP.

Refer to [Registering Devices on RAMP](#) for more information on device registration.

Customize the Alarm Interface

RAMP administrators have a wide range of controls to determine which alarm data users see in their FM user interface. Administrators can configure multiple Views and Charts to provide the optimal set of alarm data for each role in fault management. Administrators then control which Views users can access through their user group assignments.

For example, an administrator can limit the alarm set to those owned by the current user or they can filter the alarm set based on the alarm acknowledgment status. They are also able to select which alarm severity levels appear in the bar charts and which types of data appear in the active alarm list.

The FM user interface provides tools to highlight when particular alarm-related situations occur. Within Views, the administrator can activate audible alarms for different alarm severity levels, to provide users with a quick indicator of the current alarm status when they open a View. When configured, a sound file plays for the highest severity level that is currently represented within the unacknowledged alarms.

Within Charts, the administrator can configure tripwire alerts which appear in the bar chart when significant conditions are detected. Rate tripwires trigger when the rate of incoming alarm exceeds a configured threshold. Alarm tripwires trigger when any of up to four selected alarms appears within the alarm set.

Refer to [Customize the Alarm Interface](#) for more information on configuring Views and Charts.

Work with Active Alarms on the FM Dashboard

FM users access active alarms from the FM Dashboard. The currently selected View determines which alarms are visible. Within a View, one or more charts encapsulate selected sets of alarms in a color-coded, bar-chart format that provides a quick visual overview of the alarm status. Clicking on the chart opens the set of alarms in a window where the user can work with them individually or in groups.

Within the alarm list, users can perform a range of actions to address alarms such as acknowledging alarms, assigning alarms to specific users, clearing alarms, or adding written comments.

Refer to [Monitor Alarms](#) for more information on working with alarms on the FM Dashboard.

View Alarm History

The FM interface also provides an Alarm History list that users can access, when needed, to review both past and current alarms.

Refer to [Work with Alarm History](#) for more information on viewing alarm history.

Reclassify the Alarm Content

Administrators have the option to modify some attributes of alarms, such as severity level or summary, to better align them with their specific network environment or to convey business-specific information to their users. These changes are reflected both when the alarm appears in the FM alarm lists and in alarms forwarded to an external destination.

Refer to [Reclassify Alarm Content](#) for more information on reclassifying alarms.

Send Email Notifications

To ensure that important fault information reaches users even when they are not logged into RAMP, administrators can configure email notifications to be sent to specified email accounts when selected alarms occur.

Refer to [Send Email Notifications for Alarms](#) for more information on configuring email notifications.

Send Alarms to an External Destination

For businesses that want to send alarms from RAMP-managed devices to an external system such as an Operations Support System (OSS), RAMP can be configured to forward alarms to specified external destinations using the SNMP protocol. The RAMP administrator specifies criteria for which alarms to forward and specifies the destination to receive the alarms. The administrator also has the option to configure FM to allow the OSS system to request a resynchronization of alarms.

Refer to [Forward Alarms to an External Destination](#) for more information on sending alarms to an external destination.

Administer Fault Management

Alarms travel from many individual devices to RAMP and can be subject to network delays or interruptions. To ensure that alarm information is current and complete, RAMP administrators can configure policies that manage synchronizing alarms between devices and RAMP that are based on the characteristics of their network. Over time, the amount of alarm data can be significant, particularly in large networks. Therefore administrators can also control when alarms are purged, taking into consideration their alarm traffic and the capacity for storage in their deployment.

Refer to [Resynchronize Alarms](#) for more information on configuring device resynchronizing controls.

Refer to [Purge Alarms](#) for more information on purging alarms.

Fault Management Workflows

Overview

The Ribbon Application Management Platform (RAMP) Fault Management (FM) service supports a range of FM tasks. The following workflows outline the main steps required to complete key FM tasks. Each step links to a page where you can obtain detailed information and procedures.

- [Manage Alarms](#) – manage alarms for a selected set of registered devices
- [Forward Alarms](#) – forward alarms to an external destination
- [Reclassify Alarms](#) – reclassify alarm severity or modify the summary information provided with an alarm
- [Configure Alarm Notifications](#) – send email notifications when certain alarms occur
- [Troubleshoot EdgeMarc Devices](#) – troubleshoot EdgeMarc devices and resource groups

Prerequisite

For all FM workflows, you must register devices with RAMP to enable monitoring and forwarding of their alarms.

Workflows

Manage Alarms

Step	Action
1	Create a View to select the devices whose alarms you want to monitor (Optionally apply filtering).
2	Use the FM Dashboard to view a summary of the alarms from the selected devices.
3	Open an alarm list to manage the individual alarms.

Forward Alarms

Step	Action
1	Configure a Filter Profile to specify which alarms to forward.
2	Configure a Forwarding Profile to specify the alarm destination.

Reclassify Alarms

Step	Action
1	Configure Reclassification Rules.
2	Use the FM Dashboard and alarm list to view the reclassified alarms.

Configure Alarm Notifications

Step	Action
1	Configure the email server on RAMP.
2	Enable sending email notifications.
3	Configure Notifications to specify which alarms trigger notifications and to which recipients.

Troubleshoot EdgeMarc Devices

Step	Action
1	View Created Rules
2	Add Rule
3	Job Status
4	Create Email Notifications for Triggers
5	EdgeMarc Alarms

Work with Active Alarms

In this section:

- [Understand the FM Dashboard](#)
 - [Views](#)
 - [Charts](#)
 - [Total and Unique Alarms](#)
 - [Audible Alarms](#)
 - [Tripwire Alerts](#)
 - [Active Alarm List](#)
 - [Pausing](#)
 - [Filtering Alarms](#)

Related articles:

- [Customize the Alarm Interface](#)
- [Monitor Alarms](#)
- [Configure FM Dashboard Administration Settings](#)
- [Clearing Alarms](#)

Use the Fault Management (FM) service to monitor fault events and view active alarms generated by registered devices. Device alarms are forwarded to the Ribbon Application Management Platform FM service. You can view these faults using the options discussed in this section.

To monitor faults in Fault Management:

- [Create Views](#) to graphically see alarm information for selected devices/device types/clusters.
- Monitor alarms using the Views created.

- Address the alarms using the functionalities the FM service provides.

Understand the FM Dashboard

To work with active alarms, users interact with the FM dashboard. The following sections provide an overview of the FM dashboard and its features:

Views

A View allows administrators and provisioners to work with alarms from the alarm database based on Resource Groups. Resource Groups are collections of managed devices that are grouped for the purpose of assigning access control policies that apply to the group. For more information, refer to [Work with Resource Groups](#).

Once you create a View, it is available for selection on the FM Dashboard. On the FM Dashboard, select a Resource Group to choose from the Views available for that particular Resource Group.

Charts

Charts are graphical representations of Views. While a View is defined for Resource Groups as a whole, a chart within a View focuses on a sub-group of devices within a Resource Group. The FM service allows you to create a maximum of 30 individual charts within a View, each of which is a customized alarm filter.

On the FM Dashboard, the color-coded bar charts provide a quick view of all the active alarms within that View.

Total and Unique Alarms

The RAMP allows you to choose to display either all instances of a particular type of alarm within a View or just the unique alarms within that View. Select either **Total** or **Unique** from the **Alarm View** option on the FM Dashboard.

Audible Alarms

The FM dashboard provides audible alarms. When you open a View, RAMP can play selected sounds that correspond to one or more selected alarm severity levels present in the View. Audible alarms are optional, but can be an immediate indicator to the user of the status of the system.

Tripwire Alerts

The FM Dashboard provides an option to highlight the occurrence of significant conditions with tripwire alerts. Tripwire alerts appear as notifications within the bar chart when specified conditions are met. The administrator defines these conditions based on the rate at which alarms of selected severity levels are occurring or when specific alarms occur.

There are two types of tripwire alerts:

- **Rate Tripwires** – The Fault Management service triggers rate tripwires when alarms of selected severity levels occur at a defined rate.
- **Alarm Tripwires** – The Fault Management service triggers alarm tripwires when specific alarms occur.

Active Alarm List

When you click on a chart the Fault Management service opens an active alarm list. Active alarm lists are a more detailed representation of alarms represented by the charts. RAMP provides options to configure this detailed, tabular representation. From a predefined list of display settings, you can decide the level of detail you want to see. Within the alarm list, you can perform several actions like acknowledging alarms, assigning alarms to specific users, clearing alarms, or adding written comments. You can perform these actions either on individual alarms or groups of alarms. RAMP also allows you to download or print the alarm list.

Note

Clear the Alarms from the RAMP DB using an option below:

- Manual clearing of Alarms using the user interface.
- Automatic clearing of Alarms when the clear is received for a problem.
- Timer-based alarms, which get cleared automatically after some time based on the timer value, set for that particular alarm.

Pausing

The FM Dashboard allows you to pause the live refresh of the displayed alarms. You can use this feature while you reconfigure Views or check an alarm in more detail.

Filtering Alarms

In addition to choosing charts for subsets of the alarms, you can further filter the alarms displayed in a View based on the alarms' ownership and acknowledgment status. For example, for a specific Resource Group, you can monitor just unacknowledged alarms assigned to you. Configure this, if required, in the View settings.

Customize the Alarm Interface

In this section:

- [Create Views and Charts](#)
- [Modify Views and Charts](#)
 - [Edit a View](#)
 - [Delete a View](#)
 - [Edit a Chart](#)
 - [Delete a Chart](#)

The Ribbon Application Management Platform (RAMP) allows you to customize the visible alarm data required by creating Views. Views define at least one bar chart to graphically display alarm information for specified devices within a specified Resource Group.

Create Views and Charts

To create a View, enter general characteristics of the View in three categories: General Info, Alarm Info, and Audible Alarms.

- General information includes a name for the View, an optional description, and the resource group or groups for which you are creating the View.
- Alarm information settings optionally filter the alarms displayed based on alarm ownership and acknowledgment status. You also choose which columns of alarm data appear when opening an active alarm list from a Chart.
- Audible Alarm settings specify whether to play selected sounds when a View is opened based on the severity level of alarms that are present.

After you enter general View characteristics, create one or more Charts for the View. A Chart specifies a sub-group of devices whose alarms are reflected in a bar chart within the View. A Chart also provides options to configure tripwire alerts.

Use the following procedure to create a View and Chart. For PSX GR deployments, create Views for both instances because Views are not shared by the instances. If the recovery PSX must become active, this ensures that a View is available.

Prerequisite

- Review the information on [Work with Active Alarms](#) to make sure you are familiar with Views and Charts.
- You require Super User or Provisioner level [privileges](#) for Fault Management to create, modify or delete Views.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > Views**.
3. Click **Add View**.
4. In the **General Info** area, enter the following information:

Field	Description
View Name	Enter a name for the View. The field accepts alphanumeric characters, spaces, dashes, underscores, and parentheses up to 32 characters.
Description (Optional)	Enter a description for the View of up to 255 characters.
Resource Groups	Select the Resource Group containing the devices you want to monitor with the view.

5. In the **Alarm Info** area, specify whether to filter alarms based on ownership and acknowledgment status and which alarm information appears in an Active Alarm list.

Field	Description
Alarm Ownership	Choose whether you want the View to display All events, only those events assigned to the FM user (Self Only), or the events assigned to the FM user plus any unassigned events (Self and Unassigned).
Alarm Acknowledgment Status	Choose whether you want the View to display only Acknowledged events, only Unacknowledged events, or All .

Field	Description
Display Columns	Choose the alarm information to be displayed in the active alarm list. Select the column display scheme for use with this view. The available schemes are: ◦ Default – columns include Alarm Name, Device Type, Device Name, Last Occurrence, and Summary. ◦ Minimal – columns include Alarm Name and Last Occurrence. ◦ Minimal2 – columns include Alarm Name, Last Occurrence, and Summary. ◦ Variation1 – columns include Alarm Name, Device Type, Device Name, Last Occurrence, and Summary. ◦ Variation2 – columns include Alarm Name, Device Type, Device Name, Last Occurrence, and Summary. ◦ Variation3 – columns include Alarm Name, Device Type, Device Name, First Occurrence, Last Occurrence, Count, and Summary. ◦ Variation4 – columns include Alarm Name, Severity, Owner, Device Type, Device Name, First Occurrence, Last Occurrence, and Count. ◦ All – columns include Alarm Name, Severity, Owner, Device Type, Device Name, First Occurrence, Last Occurrence, Count, and Summary.

6. (Optional) In the **Audible Alarms** area, select audible alarm tones for one or more of the listed alarm severities. RAMP plays the selected alarm tone when you open the View on the FM Dashboard if alarms of that severity are present.
7. Click **Add Chart** to create a new graphical bar for the View.
8. In **Chart Name**, enter a name for the Chart.
9. In the **Devices** area, specify whether you want to select a group of devices for the Chart based on **Device**, **Cluster**, or **Device Type**.
10. Move devices from the **Available** to the **Selected** list to include their alarms in the Chart.
11. (Optional) Configure a **Rate Tripwire** for the Chart. RAMP adds a tripwire alert to the Chart if the rate of alarms for selected severities exceeds your specified limit. To configure a **Rate Tripwire**:
 - a. Select the **Tripwire will be activated for selected severities if** checkbox.
 - b. Specify the alarm rate that triggers the tripwire.
 - c. Select the severities for which you want to activate Rate Tripwires from the **Severity Table**.
12. (Optional) Configure an **Alarm Tripwire** for the Chart. RAMP adds a tripwire alert to the Chart when any of the selected alarms are present. To configure an **Alarm Tripwire**, move alarms from the **Available Alarms** to the **Selected Alarms** list using the arrow buttons.
13. Click **Save** to save the Chart and close the **Add Chart** window.
14. Repeat steps 6 to 12 until you have added all of the Charts you want to include with the View.
15. Click **Save**.

Modify Views and Charts

Edit a View

To edit an existing View:

1. Navigate to **Observability > Fault Management > Views**.
2. In the Views list, click on the View to edit.

3. Make required changes to the View settings.
4. Click **Save**.

Delete a View

To delete an existing View:

1. Navigate to **Observability > Fault Management > Views**.
2. Select **Delete** from the Actions list for the View you want to delete.
3. Confirm the deletion when prompted.

Edit a Chart

To edit an existing Chart:

1. Navigate to **Observability > Fault Management > Views**.
2. In the Views list, click on the View that contains the Chart you want to edit.
3. In the **Charts** list, click on the name of the Chart to edit.
4. Make the required changes to the Chart settings.
5. Click **Save**.

Delete a Chart

Note

The Fault Management Views automatically deletes a chart from the **Views** if there is only one node associated to a chart and that node is deleted.

The Fault Management Views automatically deletes a chart from the **Views** if there is only one cluster associated to a chart and that cluster is deleted.

When a chart is deleted automatically in such circumstances and the **View** does not have any other associated chart, then the View is deleted automatically.

To delete an existing Chart:

1. Navigate to **Observability > Fault Management > Views**.
2. In the Views list, click on the View that contains the Chart you want to delete.
3. In the **Charts** list, select **Delete** from the Actions list for the Chart you want to delete.
4. Confirm the deletion when prompted.

Monitor Alarms

Use the FM Dashboard to view a graphical representation of real-time alarms. On the FM Dashboard, select a resource group and choose from the list of available views to display the stacked bar charts showing the alarm sets. The system updates the charts at regular intervals if new alarms occur that impact the current view. Use the FM Administration view to set the update frequency. If the audible alarms are provisioned and alarms with the configured severity exist, an alarm triggers when you open the View mode. Click any chart to open a detailed alarms list chart to examine for specific alarm information. This allows you to actively manage real-time alarms using several functionalities.

Note

The Application Server (AS) does not support unacknowledged alarms and manual clear operations for outstanding alarms. If you perform any of these operations on the RAMP GUI for AS alarms, they are only performed on RAMP and are not updated on the AS.

Use the following procedure to use the FM Dashboard to process alarms:

Start

1. Log on to the RAMP GUI and navigate to **Observability > Fault Management > FM Dashboard**.
2. Select the Resource Group for the devices whose alarms you want to monitor.
3. Select the View that presents the alarms for the resource group with the filters and options you desire. If you do not configure Views, consult the person in your organization responsible for configuring Views. Each View can contain a maximum of 30 bar charts, each of which is a customized alarm filter.
4. On the FM Dashboard, perform the following actions to control your alarm view:
 - a. **Pause live refresh**—By default, the View charts update with any new alarm every 15 seconds. Click the pause icon next to **Live** to pause the updates. This allows you to examine a static chart.
 - b. **Change the view to show total or unique alarm counts**—Select the **Total** or **Unique** options to view the total number of active or unique alarms.
 - c. **Modify a View**—You can edit the RAMP Views on the FM Dashboard. To modify a View, click the name of the underlined View. For more information, refer to [Customize the Alarm Interface](#). A Super User privilege is mandatory to modify a View.
5. Each View is represented by a chart or several charts. Click on a chart to open a window with a tabular list of all the alarms associated with that chart. The alarm list, by default, contains information such as the alarm name, severity, acknowledgment status, name and type of the device that raised the alarm, date and time of the last occurrence, and a brief summary.
6. The following alarm list options are available:
 - a. **View individual alarm details**—Click an alarm name or select **Details** from the **Actions** list to open a window with more information about the selected alarm.
 - b. **Acknowledge an alarm**—Manually acknowledge an alarm so that it no longer appears in any alarm list that filters acknowledged alarms.
 - i. For any additional alarms of this type, do not change the acknowledged state of the alarm.
 - ii. Select **Acknowledge** from the **Actions** list or on the individual alarm details window.
 - iii. You can also select multiple alarms and acknowledge them using **Bulk Actions**.
 - c. **Unacknowledge an alarm**—Change the state of an Acknowledged alarm by manually changing the acknowledged state.
 - i. Select **Unacknowledge** from the **Actions** list or on the individual alarm details window.
 - ii. You can also select multiple alarms and unacknowledge them using **Bulk Actions**.
 - d. **Clear an alarm**—Clearing an alarm removes it from the database and all alarm lists.
 - i. Any journal entries added for this alarm are lost.
 1. Only new instances of this alarm appear in the alarm list.
 2. Select **Clear** from the **Actions** list on the individual alarm details window.
 3. You can also select multiple alarms and clear them using **Bulk Actions**.
 - e. **Add a comment**—Add a comment or journal entry for an alarm.
 - i. Once you enter a comment, it will appear as a Journal Entry in the alarm details window.
 - ii. Select **Comment** from the **Actions** list or enter your comment in the **Journal Entries** field in the individual alarm details window.
 - f. **Assign ownership**—Use this option to assign ownership of a selected alarm to a selected user.
 - i. Once you assign ownership, only the administrator and assigned owner can update the alarm (acknowledge, unacknowledge, comment, and clear).
 - ii. You must have either Super User or Provisioner level access to assign alarms to other users.

- g. **Clear with Forward**—Use this option to select alarms to clear from the internal database and forward the Clear Alarm/Event to the northbound customer. The Alarm History displays the cleared alarms.
- You can select up to 200 alarms.
 - If you select more than 200 alarms, a warning message notifies you that the "Clear with Forward" action will not be performed because you exceeded the 200 alarm limit.
The operation is allowed once the number of alarms are reduced to 200 or less.

The FM service also provides the following options to help you efficiently work with alarms in an alarm list:

Option	Description
Wrap	Select Wrap to word-wrap fields. This makes the table more compact and eliminates the need for horizontal scrolling.
Pause/Live	Click Pause adjacent to Live to pause the live refresh of the selected alarm list corresponding to a chart. - When paused, the Last Update box displays the time the View was last updated. - Click Play adjacent to Pause to re-enable updates. The system updates the View with any cached alarms from the period when the display was paused. Pause is automatically enabled when you select one or more alarms in an alarm list. You cannot enable the view again until all options are cleared.
Export Table	Click the ellipses at the top right corner of the pop-up dialog and select Export Table to export the list of alarms. The Export Table Data pop-up then displays. - Provide details such as Filename, File Format, Delimiter, Page, Current Option, and Limit Records. - Click Submit to export the list of alarms to your local machine.
Help	Select Help from the Actions menu to get more information about specific alarms on the alarm list. The Trap Guide opens with a description for each alarm. You can add company-specific comments and links to supporting online documentation for each Ribbon and third-party alarm listed in the Trap Guide. All users can view these comments.

Configure FM Dashboard Administration Settings

The Ribbon Application Management Platform (RAMP) allows you to configure administrative settings for the **FM Dashboard**. Configure ownership policies to decide if you want users to be able to perform operations on owned alarms only and set limits on the maximum number of alarm lists that all users on a server can open simultaneously.

Prerequisite

Super User [privileges](#) for Fault Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > Administration**.
3. In the **FM Dashboard** section on the **Administration** page, select the **Allow operations on owned alarms only** checkbox to configure the ownership policy. This option specifies whether or not users are allowed to perform operations on alarms assigned to other users, limiting users' access to alarms they own.
4. Under **Alarm List Limits**, configure the **Maximum per server** and **Auto Refresh Interval (in seconds)**. These options set an overall server limit on the number of alarm lists all users can open simultaneously and the live refresh interval for alarms.
5. Select the **Alarms For Disabled Devices** checkbox to display alarms and their counts for disabled devices that are unregistered and partially registered:
 - a. If enabled, the alarms generated for devices in an Unregistered, Partially registered, or Prepared Recovery state are displayed in the **FM Dashboard** Event list, **Home Dashboard**, and the **Resource Group Dashboard Alarm** section.
 - b. If disabled, the alarms generated for devices in an Unregistered, Partially registered, or Prepared Recovery state are not displayed in the **FM Dashboard** Event list, **Home Dashboard**, and the **Resource Group Dashboard Alarm** section.

Clearing Alarms

The following alarm-clearing options are available on the RAMP:

- Manually – The user clears the alarm using the UI.
- Automatically – The alarm clears when the 'Clear' alarm triggers after the problem is resolved.
- Timer-based alarms – The alarm clears once the configurable timer value is reached.

The RAMP includes the following configurations and default values in the `/opt/fm/conf/correlator/bootstrap.properties` file. Changing these values requires a correlator process restart.

1. To discard all old alarms during startup whose timer has expired. This is more than the configured threshold in the state store (By default, the value is 240 minutes). The alarms that cross (240*60 + timer value in seconds) are cleared.

```
StreamsConfig.timer.alarms.discard.threshold.minutes=240
```

2. To discard old alarms that cross the threshold.

```
StreamsConfig.timer.alarms.discard.old=true
```

3. To limit the maximum number of alarms cleared, send them to the DB and then forward them one at a time. If any changes are made, the correlator must be restarted.

```
StreamsConfig.timer.alarms.max.clear.count=750
```


Changing these values is not recommended since they were defined after extensive testing.

Ribbon recommends performing all UI trap operations within 30 minutes of starting the process. This applies to all upgrades from releases prior to RAMP 24.09 to RAMP 24.09 onwards.

Work with Alarm History

The Alarm History window allows you to view all the archived alarms stored in the Ribbon Application Management Platform (RAMP) database. This provides a record of alarm history for nodes registered with RAMP. All users can view the alarm history. Make sure that you purge the alarm history regularly so that it doesn't get too large. Refer to [Purge Alarms](#) for more information on purging alarms.

To view the alarm history, navigate to **Observability > Fault Management > Alarm History**.

Purge Alarms

In this section:

- [Automatic Purge](#)
- [Manual Purge](#)

The Ribbon Application Management Platform (RAMP) allows you to purge active and historical alarms you no longer need. This prevents the accumulation of large amounts of alarm data over time. You can choose when to purge the alarms depending on the size of your network, your alarm traffic, and your storage capacity.

Automatic Purge

Use the following procedure to schedule an automatic purge of old or unwanted alarms from the fault database.

Note

By default, the Fault Management automatic purge frequency for active alarms is set to "Daily" with a start time of "01:00", and the automatic purge frequency for historical alarms is set to "Hourly" with a start time of "01:00".

Prerequisite

- **Super User** [privileges](#) under **Fault Management** to purge alarm data.

Start

1. Log onto the RAMP GUI.

2. Navigate to **Observability > Fault Management > Administration**.
3. In the **Alarm Schedule Purge** area, select a Frequency (**Hourly**, **Daily**, or **Weekly**) for the purge.
 - a. You can also disable automatic purges by selecting **Disable**.
4. Set the Start time, and then select a **Start Day** (If the Frequency is **Weekly**) and select a time (hour: minute) for the purge to occur.
5. Select **Active** or **History** from the Alarms list depending on whether you want to clear active or historical alarms.
6. Specify the purge criteria by doing one of the following:
 - a. Select the **Older than** checkbox and enter a value in hours. In this case, when the purge job runs, it automatically removes all events of the selected severity level(s) older than the designated value.
Or
 - b. Select the **Max number of alarms** checkbox,.
 - c. Select a **Purge To** percent (50%, 75%, or 90%) and enter a value in the **of max size** field.
 - i. In this case, if the number of events in the database exceeds the maximum setting, the system determines the number of events that should remain in the database (maximum number of alarms * purge to percent) after the purge.
 - ii. The purge job then runs deleting events of the selected severity level(s), from oldest to newest, until it reaches the desired quantity of remaining events.
 - iii. If the number of events in the database does not exceed the maximum setting, the purge job does not run.
7. In the "Severity of alarms to purge" area, select the severity level(s) you want the purge job to remove.
8. Click **Save** to save your settings.

Manual Purge

Use this procedure to manually purge old or unwanted alarms from the Fault database:

Prerequisite

- **Super User** [privileges](#) under **Fault Management** to purge alarm data.

Start

1. Log onto the RAMP GUI.
2. Navigate to **Observability > Fault Management > Administration**.
3. In the **"Alarm Manual Purge"** area, select **Active** or **History** from the Alarms list, depending on whether you want to clear active or historical alarms.
4. Click **Time earlier than** to open a Date/Time control where you can set a base date and time. The system purges all alarms (of the types selected in the next step) that are older than the base date and time.
5. In the **Severity** area, select the types of alarms to purge. You must specify at least one type.
6. Click **Purge active alarms** to purge the records.
7. When prompted, confirm that you want to purge the alarms.

Ribbon recommends performing all UI operations on the traps 30 minutes after starting the process. This applies to all upgrades starting with 24.09 and does not apply if the older release version is already 24.09.

Reclassify Alarm Content

The Ribbon Application Management Platform (RAMP) allows you to reclassify the severity, class, and description fields displayed in the alarm lists by creating reclassification rules. This allows you to classify alarms according to your network requirements.

When you create or modify a reclassification rule, the new rule applies only to new alarms, not to alarms already received.

Prerequisite

You require Super User level [privileges](#) for Fault Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > SNMP > Reclassification Rules**.
3. To create a new rule, click **Add Rule**.
4. Enter the following information:

Field	Description
MIB	Select the MIB corresponding to the device for which you want to configure a reclassification rule.
Trap Names	Select the trap to which you want to apply the rule. Note: To see definitions of the traps or to set custom comments for a trap, click Trap Guide .
Severity	Select the severity to apply to the selected trap, or leave as "system-defined."
Class	Select the class to apply to the selected trap, or leave as "system-defined."
Summary	To add a custom description for the selected trap, clear the Use system defined Summary check box and enter your description.
Enable	Select checkbox to enable the new reclassification rule.

5. To save the alarm rule click **Save**.

To edit an existing rule, select the alarm rule you want to edit from the list and apply your changes using the preceding table.

To delete an existing rule, click the delete icon corresponding to the alarm rule you want to delete.

Send Email Notifications for Alarms

Related articles:

- [Enable Sending Alarm Notifications](#)
- [Configure Alarm Notifications](#)

The Ribbon Application Management Platform (RAMP) allows you to send alarm notifications through email. This notifies network operators or administrators of specific alarms even when they are not connected to the application. This ensures that critical network problems are not missed.

Note

Alarm notification through email is disabled by default.

Complete the following steps to set up email alarm notifications:

1. Obtain your email server IP address from your email administrator. Use this IP address as the email server for RAMP.
2. Enable alarm notifications through email on RAMP. Refer to [Enable Sending Alarm Notifications](#).
3. Send a test notification to confirm connectivity between RAMP and the mail server. This ensures that alarm notifications are not blocked. If you do not receive email notifications, check with your email administrator. Refer to [Enable Sending Alarm Notifications](#) for the procedure to send test notifications.
4. Set your email source address. Refer to [Enable Sending Alarm Notifications](#) for the procedure to set a source address.
5. Configure email alarm notifications on RAMP to specify which alarms trigger emails and to whom they are sent. Refer to [Configure Alarm Notifications](#).

Enable Sending Alarm Notifications

The Alarm notifications through email are generated on RAMP and relayed to a mail server (SMART_HOST). It is the mail server configured to accept relaying from the RAMP server and to further process incoming messages from the RAMP server.

The administrator of the remote mail server (SMART_HOST) must configure the mail server to accept emails from the RAMP server.

Prerequisites

- You require Super User [privileges](#) for Fault Management.
- You require the IP address of an email server in your network to handle relaying RAMP email notifications.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > Administration**.
3. In the **Email Notification** area, select the **Schedule Notification** checkbox.
4. You can also set the notification frequency by entering the required time in the **Notification Frequency (in minutes)** field.
5. Click **Save**.
6. Log on to the RAMP CLI as the root user. Refer to [Log onto the RAMP CLI](#).
7. Issue the following command to add the mail server. If RAMP will be deployed in a GR configuration, run the command on the active instance after setting up the GR configuration.

```
/opt/sonus/ems/conf/enableEmailNotification.sh <SMART_HOST IP address>
```

8. Set your email source address:

- a. Navigate to **Observability > Fault Management > Notifications**.
- b. Click **Edit** adjacent to **Email Source Address**.
- c. In the **Email Address** field, enter an email address.
- d. Click **Save**. This email address is used as the "From:" header field as per RFC5322.
9. Send a test notification to confirm connectivity between RAMP and the mail server.
 - a. Navigate to **Observability > Fault Management > Notifications**.
 - b. Enter an email addresses in the **Send a Test Notification to email address** field.
 - c. Click **Send**. A success message is displayed once a test notification is sent.

Configure Alarm Notifications

In this section:

- [Add a Notification](#)
- [Edit a Notification](#)
- [Delete a Notification](#)

Configure email alarm notifications on Ribbon Application Management Platform (RAMP) to choose which alarms trigger email notifications and when they trigger them. In a notification, you also choose who to send email notifications to. You can configure multiple recipients to receive email alarm notifications.

RAMP sends alarm notification emails at predefined intervals in an HTML format. If multiple alarms occur during the interval they are grouped into a single email. Duplicate alarms are suppressed; if there are multiple alarms of the same type, the alarm is mentioned only once in an email. The subject of the emails includes the alarm count.

You can filter alarms based on the criteria set in a notification and **RAMP** send emails automatically.

Add a Notification

Use the procedures in this section to add a notification.

Prerequisite

You require Super User [privileges](#) for Fault Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > Notifications**. The **Notifications** window opens.
3. Click **Add Notification**.
4. Enter the following information to define a set of criteria that trigger an email notification:

Field	Description
Notification Name	Enter a name for the notification.
Email Addresses	Enter the recipient email addresses to receive emails for this notification. You can specify multiple e-mail addresses. Separate e-mail addresses with commas.
Severity	Select the alarm severity levels for which you want RAMP to generate emails from this notification.

Field	Description
Select Network Element via	Select one of the following options to specify which devices' alarms will trigger emails for this notification: ◦ Type – Select Type to select devices by device types. The Cluster / Node Type list appears for you to select the device types. ◦ Resource Group – Select Resource Group to select devices by specific Resource Groups. The Resource Group list appears for you to select the Resource Groups. ◦ Specific Element – Select Specific Element to select devices by name. The Specific Clusters and Specific Nodes lists appear for you to select the devices.
Alarm List	Select the triggering alarms from the Alarm List . The list of alarms available is filtered by your device selection.
Time Frame Use the Time Frame options to either specify times during which the email-triggering rules will apply, or to specify that the rules apply at any time.	
Any Time	Select this checkbox to receive alarm notifications for alarms occurring anytime. The other time frame options are disabled.
Only alarms between On these days	Select the time range during the day and the days of the week during which you want to receive alarm notifications if triggering alarms occur. Enter a start and end time, and select the days.
Alarm Information	
Info included in notification	Select the alarm fields to be displayed in the alarm notifications.
Notification Description	Enter any additional text to include in the email notification along with the alarm information. This text appears in the notification email.

5. Click **Save** to save the notification.

Edit a Notification

To edit an existing notification:

1. Navigate to **Observability > Fault Management > Notifications**.
2. In the Notifications list, click on the notification to edit.
3. Make required changes to the notification settings.

4. Click **Save**.

Delete a Notification

To delete an existing notification:

1. Navigate to **Observability > Fault Management > Notifications**.
2. Select **Delete** from the Action list for the notification you want to delete.
3. Confirm the deletion when prompted.

Forward Alarms to an External Destination

In this section:

- [Configure Forwarding Criteria in a Filter Profile](#)
- [Configure the Alarm Destination in an Export Profile](#)
- [Modify Existing Profiles](#)
 - [Edit a Filter Profile](#)
 - [Delete a Filter Profile](#)
 - [Edit an Export Profile](#)
 - [Delete an Export Profile](#)

Related articles:

- [Resynchronize Alarms](#)

You can configure Ribbon Application Management Platform (RAMP) to forward alarms to third-party applications. A RAMP administrator creates forwarding profiles to specify which traps to forward and where to send them. RAMP also allows you to configure Trap Resync to ensure that no alarms are missed, in case of a network or device failure. Refer to [Resynchronize Alarms](#).

To forward alarms, create the following type of forwarding profiles:

- Filter Profile – Filter Profiles determine what types of alarms from which source addresses are forwarded.
- Export Profile – Export Profiles determine the export parameters for alarms.

Configure Forwarding Criteria in a Filter Profile

Use the following procedures to create a filter profile that specifies trap forwarding criteria.

Prerequisite

You require Super User [privileges](#) for Fault Management to create, modify or delete forwarding profiles.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > SNMP > Forwarding Profiles**.
3. Select the **Filter** tab.
4. Click **Add Filter Profile**.
5. Enter the following information:

Field	Description
Profile Name	Enter a name for the filter profile.

Field	Description
Description (Optional)	Enter a description for the profile.
Filter Profile Enabled	Select this checkbox to enable/activate this filter profile.
Nodes/Nodes Types/Clusters Available	Select the source nodes/node types/clusters for the alarms that you want forward.
Trap Type Filter Set values for at least one of the following to determine which traps to forward.	
Types Available	Select the traps to forward from the list.
Severity	Select the severity levels of the alarms to forward.
Alarm Class	Select the classes of the alarms to forward.

6. To save the Filter Profile, click **Save**.

Configure the Alarm Destination in an Export Profile

Use the following procedures to create an export profile that specifies export parameters for alarms and the alarm destination.

Prerequisite

You require Super User [privileges](#) for Fault Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > SNMP > Forwarding Profiles**.
3. Select the **Export** tab.
4. Click **Add Export Profile**.
5. Enter the following information:

Field	Description
Profile Name	Enter a name for the export profile.
Description (Optional)	Enter a description for the profile.
Associated Filter Profile	Select a filter profile to associate with the export profile. Only enabled filter profiles are shown in the list.
Export Profile Enabled	Select this checkbox to enable/activate this export profile.

Field	Description
Maximum Rate	Select the maximum number of traps to be forwarded per second.
OSS Resync Enabled	Select this checkbox to enable OSS Trap Resync. Refer to Resynchronize Alarms for more information about OSS Trap Resync.
Data Format	Specifies the data format in which the traps are forwarded. Note: Only the SNMP data format is available.
IP Address	Enter the IP address of the destination to receive the traps
Port	Enter the port number to use at the destination.
Version	Select the SNMP Trap version from the following options: ◦ SNMP v1 – If you select SNMP v1, enter a community string. By default, it is "public". ◦ SNMP v2c – If you select SNMP v2c, enter a community string. By default, it is "public". ◦ SNMP v3 (default) – If you select SNMP v3, select a security levels from the Security Level list:
Security Level	This parameter is applicable only for SNMPv3. If you select SNMPv3, select one of the following security levels from the Security Level list: ◦ NoAuthNoPriv – users that connect with this level have no authentication, and the messages they send and receive are not private. ◦ AuthNoPriv – connections that use this model must authenticate, but the messages are sent without any encryption. ◦ AuthPriv – authentication is required, and messages are encrypted.
Community	The parameter is applicable only for SNMP v1. Enter a value for the SNMP community string. A value is set by default.

Field	Description
Username	The parameter is applicable only for SNMP v3. Enter a username for authentication.
SNMP v3 Authentication Protocol	This parameter is applicable only if Security Level is set to one of the following: ◦ AuthNoPriv ◦ AuthPriv Select a Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol from the following: ◦ DES ◦ AES128 ◦ AES192 ◦ AES256
Auth Password	The parameter is applicable only if Security Level is set to one of the following: ◦ AuthNoPriv ◦ AuthPriv Enter a password for authentication. The minimum member of characters required for the password is as follows: ◦ DES: 8 ◦ AES128: 16 ◦ AES192: 24 ◦ AES256: 32

Field	Description
SNMP v3 Privacy Protocol	The parameter is applicable only if Security Level is set to AuthPriv. Privacy protocols enable private interactions over secure channels. Select a Message Digest (MD5), Secure Hash Algorithm (SHA), or Hash-Based Message Authentication Code (HMAC) from the following: ◦ MD5 ◦ SHA ◦ HMAC128SHA224 ◦ HMAC192SHA256 ◦ HMAC256SHA384 ◦ HMAC384SHA512
Priv Password	The parameter is applicable only if Security Level is set to one of the following: ◦ AuthNoPriv ◦ AuthPriv Enter a password for authentication. The minimum number of characters required for the password is as follows: ◦ MD5: 16 ◦ SHA: 20 ◦ HMAC128SHA224: 28 ◦ HMAC192SHA256: 32 ◦ HMAC256SHA384: 48 ◦ HMAC384SHA512: 64
Normalize alarms	Select this checkbox to normalize alarm forwarding. If enabled, all alarms are forwarded to upstream systems in a standard format.
Add device hostname to alarms	Select this checkbox to add device hostnames to forwarded alarms. Note: This option is not available if alarms are normalized.
Add epoch oid to alarms	Select this checkbox to add sonusSequenceEpoch variable binding (varbind) in the forwarded traps. Clear this check box to exclude sonusSequenceEpoch varbind from the forwarded traps. Note: This option is not available if alarms are normalized.

Field	Description
Enable single device source address	Select this checkbox to use a single IP address as the source address when forwarding traps for nodes with multiple IP addresses. The system displays the IP address from the Default IP Address field of the device's Node Information. ◦ Traps received on any of the IP addresses registered in RAMP forward through the first IP address in the host. ◦ Traps received on an IP address that is not registered in RAMP forward through the same IP address. ◦ Traps received on a logical IP address forward through the same logical IP address.
Enable loop checking	Select this checkbox to check whether a received trap has already been forwarded. If the trap forwarder determines the trap was previously forwarded, it does not forward it again. This check eliminates the possibility of two systems forwarding the same trap back and forth.

6. To save the Export Profile, click **Save**.

Once you create a filter profile and export profile, forwarding of alarms matching the profile criteria begins immediately.

Modify Existing Profiles

Use the following procedures to edit or delete existing profiles.

Edit a Filter Profile

To edit an existing filter profile:

1. Navigate to **Observability > Fault Management > SNMP > Forwarding Profiles**.
2. Select the **Filter** tab.
3. In the Filter Profiles list, click on the filter profile to edit.
4. Make required changes to the filter profile settings.
5. Click **Save**.

Delete a Filter Profile

To delete an existing filter profile:

1. Navigate to **Observability > Fault Management > SNMP > Forwarding Profiles**.
2. Select the **Filter** tab.
3. Click the Delete icon corresponding to the filter profile you want to delete. You cannot delete a filter profile associated with an export profile.
4. Confirm the deletion when prompted.

Edit an Export Profile

To edit an existing export profile:

1. Navigate to **Observability > Fault Management > SNMP > Forwarding Profiles**.
2. Select the **Export** tab.
3. In the Export Profiles list, click on the export profile to edit.

4. Make required changes to the export profile settings.
5. Click **Save**.

Delete an Export Profile

To delete an existing export profile:

1. Navigate to **Observability > Fault Management > SNMP > Forwarding Profiles**.
2. Select the **Export** tab.
3. Click the Delete icon corresponding to the export profile you want to delete.
4. Confirm the deletion when prompted.

Resynchronize Alarms

In this section:

- [Enable and Configure Device Trap Resync](#)
- [Configure Resyncing Traps from RAMP to the OSS](#)
- [Edit Trap Resync Settings](#)
- [Delete Trap Resync Settings](#)

Along with trap forwarding, the Ribbon Application Management Platform (RAMP) also allows you to configure Trap Resync parameters to enable retrieving alarms from registered devices to ensure that no alarms are missed in case of a network or device failure.

RAMP supports a northbound interface to synchronize active alarms with an upstream operations support system (OSS). When the OSS sets a specific varbind (OID) on the northbound MIB, RAMP triggers alarm synchronization based on the export profile.

RAMP also supports a southbound interface for synchronizing alarms with registered devices. RAMP maintains the sequence number of forwarded traps and provides a user interface to enable system-wide trap resynchronization for managed devices with trap history support. If there is a trap loss and trap resynchronization is enabled, the Fault Management service retrieves the lost traps stored in the corresponding devices. When trap resynchronization is enabled and no traps are received from a device for a configurable idle time period, the Fault Management service queries the device for the sequence number of the last trap sent and compares it with its record of the last received trap from the device. If there is a mismatch, RAMP consider it a loss of traps and it retrieves the lost traps.

Note

Some traps might be present in DSC and appear on the RAMP Dashboard, even when cleared. Clear these alarms manually.

Enable and Configure Device Trap Resync

Trap Resync is disabled by default. Use the following procedure to enable it and configure trap resync parameters.

Prerequisite:

Super User level [privileges](#) for Fault Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > Administration**.
3. In the **Process** area, enable trap resync by selecting the **Enable Trap Resync (from supported devices)** checkbox.
4. Enter the following information to configure the resync parameters:

Field	Description
Max no. of traps to resync	Enter the maximum number of traps RAMP can resynchronize at a time.
Max no. of resync retries	Enter the maximum number of retries the Fault Management service can attempt to resync in the event of failures.
Resync connection timeout (in secs)	Enter the timeout limit when the initial REST connection is being made.
Max no. of alarms per state-sync request	Enter the maximum number of alarms allowed in one REST request to the device during a bulk state-sync operation like acknowledge/clear/comment.
Resync read timeout (in secs)	Enter the wait period before timing out when reading data from the device.
Trigger Proactive Resync every _ seconds	Enter the time duration after which RAMP proactively queries for traps from managed devices.
Trap retention period on device (in minutes)	To support lost trap recovery, each node stores the traps in its database for a configurable time period, starting from the time the trap is generated. This time period is termed as the trap retention time period. The default value of Trap Retention Time Period is 120 minutes and the valid range is 0 to 120 minutes.

5. Click **Save** to save the parameter configuration.

Configure Resyncing Traps from RAMP to the OSS

Configure OSS trap resync to resync alarms from **RAMP to the OSS**.

Create trap resync settings for **RAMP** to trigger alarm synchronization based on the forwarding profile. Alarm synchronization is supported for regular and normalized alarms. If the alarm synchronization with the OSS is disrupted, **RAMP** does not retry alarm synchronization.

Alarm resync between an OSS and RAMP is not supported for SNMP v1.

Prerequisite:

Super User [privileges](#) for Fault Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > Administration**.
3. In the **Process** area under **OSS Trap Resync**, enter the following information:

Field	Description
Resync Port	Enter the port to which the OSS resync agent is bound for processing SNMP set-requests from authorized OSS clients. The default port number is 1161.
Oss Resync EngineId	Specifies the SNMP engine ID of the OSS resync agent. This is used by the OSS clients while sending SNMP set-requests.
Authoritative EngineId	Specifies the SNMP engine ID that is set in the SNMP traps that are forwarded to the OSS.

4. Click **Save**.
5. To create trap resync settings, navigate to **Observability > Fault Management > SNMP > OSS Trap Resync**.
6. Click **Add Resync Setting**.
7. Enter the following information:

Field	Description
SNMP Version	Select the SNMP Trap version from the following options: ◦ V2 – Select V2 for SNMP v2. ◦ V3 – Select V3 for SNMP v3. The other fields mentioned in this table appear based on your SNMP Version selection.
OSS IP Address	Enter the IP address of the OSS. IPv4 and IPv6 formats are allowed.
SNMP Write Community	This field appears when you select V2 as the SNMP Version. Enter the community string to send for the SNMP set-request by the OSS. The character length should be between 8 and 32.
Security Name	This field appears when you select SNMP V3 version. Enter a name for the SNMP v3 user for the OSS. The character length should be between 8 and 32.

Field	Description
Security Level	This menu appears when you select V3 as the SNMP Version. select one of the following security levels from the Security Level list: ◦ NoAuthNoPriv ◦ AuthPriv i. In the Authentication Protocol field, select an authentication protocol. ii. In the Authentication Passphrase field, enter an authentication passphrase. The character length should be between 8 and 32. iii. In the Privacy Protocol field, select a privacy protocol. iv. In the Privacy Passphrase field, enter a privacy passphrase. The character length should be between 8 and 32. ◦ AuthNoPriv i. In the Authentication Protocol field, select an authentication protocol. ii. In the Authentication Passphrase field, enter an authentication passphrase. The character length should be between 8 and 32.

8. Click **Save** to save the resync setting.

Edit Trap Resync Settings

To edit an existing trap resync setting:

1. Navigate to **Observability > Fault Management > SNMP > OSS Trap Resync**.
2. In the resync settings list, click **resync setting** to edit.
3. Make the required changes to the trap resync setting. You cannot edit the OSS IP address after creating a Resync Setting. To modify the OSS IP address, delete the Resync Settings and create another one with the new IP address.
4. Click **Save**.

Delete Trap Resync Settings

To delete an existing trap resync setting:

1. Navigate to **Observability > Fault Management > SNMP > OSS Trap Resync**.
2. Click the Delete icon corresponding to the resync setting you want to delete.
3. Confirm the deletion when prompted.

Monitor Fault Management Activity

The Ribbon Application Management Platform (RAMP) allows you to monitor Fault Management activity that may impact the application's performance or storage.

Prerequisite

You require Super User level [privileges](#) for Fault Management.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > Administration**.
3. Scroll down to the **Present Usage** section.
4. The following information is displayed:
 - **Number of active alarm records** – This shows the total number of alarms in the active alarms record. This includes cleared alarms.
 - **Number of alarm history records** – This shows the total number of alarms in historical table.
 - **Number of alarm lists currently open across Insight** – This shows the total number of alarm lists opened currently by RAMP users.
5. To update the information with current numbers, click the **Refresh** button.

Troubleshooting Guide

This guide provides troubleshooting advice for the Ribbon Application Management Platform (RAMP) and the devices it manages.

In this section:

- [EdgeMarc Troubleshooting](#)
 - [Create Trigger Notification Rules for EdgeMarc Devices](#)
 - [Troubleshooting EdgeMarc Devices](#)
- [Database Troubleshooting](#)
 - [Cleaning Debezium Data](#)
 - [Start DBaaS Service in RAMP](#)
 - [Stop DBaaS Service in RAMP](#)
- [Fault Manager Troubleshooting](#)
- [General Troubleshooting](#)
- [GSX Troubleshooting](#)
 - [GSX Navigator Troubleshooting](#)
 - [GSX Upgrade Troubleshooting](#)
- [RAMP CNF Troubleshooting](#)
- [RAMP GR Auto-Switchover Troubleshooting](#)
- [Retrieve System Information](#)
- [Tools Troubleshooting](#)
- [Unlock or Recover a User Account for Sysadmin or Any Admin User](#)

EdgeMarc Troubleshooting

Use this section to troubleshoot EdgeMarc devices managed by the Ribbon Application Management Platform (RAMP).

In this section:

- [Create Trigger Notification Rules for EdgeMarc Devices](#)
- [Troubleshooting EdgeMarc Devices](#)
 - [View EdgeMarc Device Analysis Details](#)

- [EdgeMarc Diagnostic Files](#)
- [Run Health Reports on EdgeMarc Devices](#)

Create Trigger Notification Rules for EdgeMarc Devices

In this section:

- [View Existing Rules](#)
- [Add a Rule](#)
- [Retrieve Ring Buffer Contents](#)
- [Create Email Notifications for Triggers](#)

Use the Ribbon Application Management Platform (RAMP) to set the threshold levels (rules) that trigger notifications for EdgeMarc devices when events occur such as Device Down, Device Up, severity of the Application Diagnostic Report, and Kernel Report. The RAMP supports creating notification triggers for either individual EdgeMarc devices or resource groups.

The EdgeView service generates and sends traps to RAMP's Fault Management when reaching the threshold condition set on the RAMP for an EdgeMarc device or resource group. These traps are listed on the [Fault Management](#) page.

Prerequisites

Super User [privileges](#) in Fault Management.

View Existing Rules

Use this procedure to view the list of existing rules.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > EdgeMarc Troubleshooting**. This dialog box lists the rules created to trigger notifications. These notifications are created based on previously defined trigger rules and actions. The columns on the **EdgeMarc Troubleshooting** page are:

Column Name	Description
Name	Name of the rule.
Severity	Severity of the rule
Applies to	Scope of the rule. When created on an EdgeMarc device, it displays the device <code>mac_address</code> . When made on a resource group, it shows the name of the resource group.
Trigger Type	The type of trigger.
Action	The action associated with the trigger.

Column Name	Description
Last Trigger	The date and time of the last trigger for a particular rule.
Status	The active or inactive state of the rule.
Actions	Edit or delete a particular rule.

Add a Rule

Use this procedure to add a rule for each EdgeMarc device or resource group to trigger and define notifications.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Observability > Fault Management > EdgeMarc Troubleshooting**.
3. Click **+Add Rule**.
4. Use the following table to add rules to trigger notifications and then click **Save**.

Note

- If you create the same type of rule for an EdgeMarc device and the resource group containing that EdgeMarc device, then the alarm is raised only for the device and not the resource group.
- Creating multiple rules of the same type on the same scope (device or resource group) is restricted. For example, you cannot create multiple **Device Down** types of rules on the same device or resource group.

Add Rule Parameters

Parameter	Description	Rule	Action	Rule Severity	Length/Range	Mandatory/Optional
Define Triggers and Actions						
Trigger Type						
Name	Provide a name for the rule.	N/A	N/A	N/A	Alphanumeric characters - and _ are allowed.	M

Parameter	Description	Rule	Action	Rule Severity	Length/Range	Mandatory/Optional
Application Diagnostic Report	This notification is triggered when the application crashes on the EdgeMarc device. The EdgeMarc device sends this crash event to RAMP and a diagnostic T-Info File containing the application crash details like stack trace, etc. RAMP accepts the T-Info file and uploads it to the configured object store. The format of the uploaded file is <code>tinfo-2023-12-27-03-59-53-472231.ev</code>. RAMP then creates a record of this file in the database. You can view, download, or delete these files. For more information, refer to EdgeMarc Diagnostic Files.	N/A	N/A	◦ Critical ◦ Major ◦ Minor ◦ Warning ◦ Intermediate The default value is "Critical".	N/A	O

Parameter	Description	Rule	Action	Rule Severity	Length/Range	Mandatory/Optional
Device Down	Notifies that the particular device is down or the devices from the resource group are down.	Notification is triggered as soon as the device is down.	The only action for this rule is notifying recipients.	◦ Critical ◦ Major ◦ Minor ◦ Warning ◦ Intermediate The default value is "Critical".	N/A	O
Device Up	Notifies that the particular device is up or the devices from the resource group are up. The default value is "Critical".	Notification is triggered as soon as the device is down.	The only action for this rule is notifying recipients.	◦ Critical ◦ Major ◦ Minor ◦ Warning ◦ Intermediate The default value is "Critical".	N/A	O

Parameter	Description	Rule	Action	Rule Severity	Length/Range	Mandatory/Optional
Kernel Diagnostic Report	This notification is triggered when the kernel crashes on the EdgeMarc device. The EdgeMarc device sends this crash event to RAMP and a diagnostic T-Info file, containing the kernel crash details. RAMP accepts the T-Info files, and uploads them to the configured object store. The format of the uploaded is:: <pre>kernellog-2023-12-20-17-10-21-256548000.ev</pre> RAMP then creates a record of this file in the database. You can view, download, or delete these files. For more information, refer to EdgeMarc Diagnostic Files.	N/A	N/A	◦ Critical ◦ Major ◦ Minor ◦ Warning ◦ Intermediate The default value is "Critical".	N/A	O

Parameter	Description	Rule	Action	Rule Severity	Length/Range	Mandatory/Optional
LAN Status Down	This notification is triggered when the LAN status changes to DOWN, The Edgemarc device sends the LAN status data to RAMP regularly. If RAMP receives the LAN information having an interface with <code>StatusChange= YES</code> and <code>Status= DOWN</code> then the rule is triggered and the SNMP alarm notification is sent to RAMP's Fault Management.	Notification is triggered as soon as the LAN Status is down.	The only action for this rule is notifying recipients.	◦ Critical ◦ Major ◦ Minor ◦ Warning ◦ Intermediate The default value is "Critical".	N/A	O

Parameter	Description	Rule	Action	Rule Severity	Length/Range	Mandatory/Optional
MOS Below Threshold	Notifies that the MOS score falls below a pre-configured threshold on an EdgeMarc device.	Specify the number of events allowed to occur over a period of time in minutes.	(Optional) Select the action to perform when the rule is triggered. For example, retrieve Ring Buffer contents for all affected devices for the period.	◦ Critical ◦ Major ◦ Minor ◦ Warning ◦ Intermediate The default value is "Critical".	Occurrences: 1 to 1000. Duration: 1 to 1500 minutes.	O
SIP Server Change	SIP Server Change is triggered due to a redundancy on the EdgeMarc device. In such instances, the EdgeMarc device switches to the next SIP server on the list or switches back to one with a higher priority.	Notifies that there is a SIP Server change.	(Optional) Select the action to perform when the rule is triggered. For example, retrieve Ring Buffer contents for all affected devices for the time period.	◦ Critical ◦ Major ◦ Minor ◦ Warning ◦ Intermediate The default value is "Critical".	N/A	O

Parameter	Description	Rule	Action	Rule Severity	Length/Range	Mandatory/Optional
SIP server Mode Change	SIP server Mode Change is triggered when an EdgeMarc device goes in or out of survivability.	Notifies that the SIP Server has a mode change.	(Optional) Select the action to perform when the rule is triggered. For example, retrieve Ring Buffer contents for all affected devices for the time period.	◦ Critical ◦ Major ◦ Minor ◦ Warning ◦ Intermediate The default value is "Critical".	N/A	O
SIP server Unavailable	This notification is triggered when an EdgeMarc device loses contact with the SIP server.	Notifies that the SIP Server is unavailable.	(Optional) Select the action to perform when the rule is triggered. For example, For all affected devices, retrieve Ring Buffer contents for the time period.	◦ Critical ◦ Major ◦ Minor ◦ Warning ◦ Intermediate The default value is "Critical".	N/A	O

Parameter	Description	Rule	Action	Rule Severity	Length/Range	Mandatory/Optional
T1 Status Down	This notification is triggered when the status of T1 changes to DOWN. The EdgeMarc device sends the T1 status data to RAMP at regular intervals. If RAMP receives T1 information having the interface <code>StatusChange= YES</code> and <code>Status= DOWN</code>, then the rule is triggered and the SNMP alarm notification is sent to RAMP's to Fault Management.	Notifies that the T1 Controller Status is down.	The only action for this rule is notifying recipients.	◦ Critical ◦ Major ◦ Minor ◦ Warning ◦ Intermediate The default value is "Critical".	N/A	O

Parameter	Description	Rule	Action	Rule Severity	Length/Range	Mandatory/Optional
WAN link Change	This notification is triggered when the WAN link changes on the device. For example, when the role of the current primary WAN is taken over by another WAN due to traffic. or vice-versa. This rule is configurable to perform an action when triggered.	Notifies that the there is a WAN Link change.	(Optional) Select the action to perform when the rule is triggered. For example, For all affected devices, retrieve Ring Buffer contents for the time period.	◦ Critical ◦ Major ◦ Minor ◦ Warning ◦ Intermediate The default value is "Critical".	N/A	O
Define Scope	Select either a resource group or the EdgeMarc device to apply the rule. ◦ Resource Group- Select the resource group to apply the rule. ◦ Device- Select the EdgeMarc device to apply the rule.	N/A	N/A	N/A	N/A	M

Parameter	Description	Rule	Action	Rule Severity	Length/Range	Mandatory/Optional
Status	Once the rule is created, it is enabled by default and the rule is implemented. Uncheck to make the rule inactive.	N/A	N/A	N/A	N/A	M

Retrieve Ring Buffer Contents

You can enable **Action** to retrieve **Ring Buffer** details while creating certain rules, for example, SIP server Change. If this rule is triggered then the diagnostic snapshot is invoked on the EdgeMarc device or the resource group. To view diagnostic snapshot refer to [Snapshot Diagnostics for EdgeMarc devices](#).

You can also view the diagnostic snapshot job on the **Job Status** page. For more information, refer to [Job Status](#). On the **Job Status** page, the **Type** column displays the type as **Rule** and the **Source** column displays the name of the rule triggering the job.

Create Email Notifications for Triggers

RAMP allows you create and send alarm notifications through email. For more information on creating email notifications, refer to [Send Email Notifications for Alarms](#).

Troubleshooting EdgeMarc Devices

In this section:

- [View EdgeMarc Device Analysis Details](#)
- [EdgeMarc Diagnostic Files](#)
- [Run Health Reports on EdgeMarc Devices](#)

The Ribbon Application Management Platform (RAMP) allows you to view details like packet capture and snapshot diagnostics, diagnostic files, and run health reports for a selected EdgeMarc device.

View EdgeMarc Device Analysis Details

In this section:

- [View Recent Calls, Packet Capture, and Snapshot Diagnostics](#)
- [Packet Capture](#)
- [Snapshot Diagnostics](#)

Use the Ribbon Application Management Platform (RAMP) to view call analysis details, including viewing and scheduling Packet Capture and Snapshot Diagnostics for selected EdgeMarc devices.

Note

Packet Capture and Snapshot Diagnostics are not supported for IPv6 addresses on the RAMP 23.12.

Prerequisites

- Posses **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- Posses **Devices, Resource Groups** [privileges](#) under **Device Management**.

View Recent Calls, Packet Capture, and Snapshot Diagnostics

Perform the following procedure to view the list of most recent calls, captured packets and snapshot diagnostics.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Devices**. The **Devices** window displays.
3. In the nodes list, click on the **Node Name** of an EdgeMarc device to view its details.
4. Click the **Analysis** tab. The **Most Recent Calls, Packet Capture, and Snapshot Diagnostics** for the selected EdgeMarc device are displayed.

Packet Capture

Perform this procedure to collect packet capture for all WAN, LAN, or both the interfaces on EdgeMarc devices through RAMP.

The EdgeMarc device stores the collected packet capture details as a single file and uploads it to RAMP. The **Status** column is updated as **Complete** when one of the conditions or parameters is met. Packet capture is allowed for a maximum duration of two days or for a maximum size of 4 GB. If the packet capture does not complete, the capture is marked as **Failed**.

Note

If you run any bulk action on the selected EdgeMarc device, then you are not allowed to run Packet Capture and Diagnostic Snapshot operations on the same device.

If PCAP or Diagnostic Snapshot operations are running, you are allowed to run any bulk action on the same EdgeMarc device simultaneously.

By default, you are allowed to run a maximum of 50 Packet Captures simultaneously on different EdgeMarc devices. You can configure the default limit from the properties file.

Start

1. Click **Start Packet Capture** to start a new Packet Capture and provide the following details:

Packet Capture stops when it runs for the specified maximum duration or accumulates the maximum size provided as input, whichever occurs first.

Parameter	Length/Range	Description
Max Duration	01m-48hrs	The maximum duration to capture the packets.
Max Size	1-4096 MB	The maximum size of each packet.
Interface		Select one of the of the following: ◦ All ◦ LAN ◦ WAN The default value is "All".
Capture Filter	Default value is "None".	Performed to capture the packets which gets transmitted over a network. There are various types, of packets that are captured. For example, some packets contain call related information, some packets contain media related information, etc. Packet Capture filter provides a way to filter packets based on our need.
Comment	Enter comments or a note for your reference.	Enter comments or a note for your reference.

- When you complete specifying the details for packet capture, click **Start** to start the packet capture.
- When packet capture starts, the **Status** column is updated as **Running**.

Note

When the status is **Running**, you are not allowed to create another packet capture for the same device. The **Start Packet Capture** button is disabled for that duration.

- The **Status** column is updated as **Complete or Failed** when one of the conditions or parameters is met. The status depends on what the device has sent. Packet capture is allowed for a maximum duration of two days or for a maximum size of 4 GB. If the packet capture does not complete, the capture is marked as **Failed**. Only when the status is either completed or failed, you are allowed to delete and download a packet capture file from the **Actions** column.

Refresh the table to see the change in the status.

- From the **Actions** column, download the packet capture file. A download is allowed only if the status is either **Complete** or **Failed**.
- You are allowed to delete a packet capture file from the **Actions** column.
- You are allowed to stop packet capture from the **Actions** column. This is possible only when the status is **Running**.

Snapshot Diagnostics

RAMP allows you to collect the diagnostic reports for that instant. When you take a snapshot from the **Analysis** tab in **Device Overview**, RAMP connects to the selected EdgeMarc device and collects the diagnostic snapshot. This report is uploaded to the RAMP's private object store. You can download this report from the **Actions** column.

Start

1. Click **Take Snapshot**.
2. The **Status** column is updated as **Running**.

When the status is **Running**, you are not allowed to take another snapshot for the same device. The **Take Snapshot** button is disabled for that duration.

3. From the **Actions** column download the snapshot when the **Status** column is updated as **Complete** or **Failed**. Download is allowed only if the status is either **Complete** or **Failed**.
4. You are allowed to delete the snapshot details from the **Actions** column.
5. You are allowed to stop snapshot diagnostics from the **Actions** column. This is possible only when the status is **Running**.

EdgeMarc Diagnostic Files

The Ribbon Application Management Platform (RAMP) allows you to view the diagnostic files for a selected EdgeMarc device. When an application crashes on the EdgeMarc device the rules specific to diagnostic reports are triggered. The EdgeMarc device sends this crash event to RAMP along with a diagnostic T-Info File, containing the application crash details like stack trace, etc. RAMP accepts the T-Info file and uploads them to the configured object store. The format of the uploaded file is: `tinfo-2023-12-27-03-59-53-472231.ev`. AMP then creates a record of this file in the database.

You can view, download, or delete these files.

Prerequisites

- **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Devices**. The **Devices** window displays.
3. In the nodes list, click on the **Node Name** of an EdgeMarc device to view its details.
4. Click the **Diagnostic Files** tab.

The **Diagnostic Files** tab displays the list of T-info files.

Run Health Reports on EdgeMarc Devices

The Ribbon Application Management Platform (RAMP) allows you to run health reports on selected EdgeMarc devices. When you run the health report for the desired devices, the attached **Devices** tab lists all the devices associated with the selected EdgeMarc device. For more information on Attached Devices, refer to [View Attached Devices for EdgeMarc](#).

Prerequisites

- **Super User** [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices, Resource Groups, and Job Status** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **Device Management > Devices**.
3. Select the EdgeMarc device to run the health report.
4. From the **Bulk Actions** menu, select **Run Health Report**. The **Run Health Report** window displays.
5. The **Included Devices** panel lists the configured EdgeMarc devices on RAMP.
6. Use the following table to update the **Frequency** to run the health report.

Parameters

Parameter	Description	Length/Range
Frequency		
One Time Only		
Perform Now	The default value is One Time Only, Perform Now .	
Perform Later	Select this option to generate health report by providing: • Date • Time	• 1 - 30 or 1- 31 depending on the calendar month. • 00:00:00 - 23:59:59
Comments	Enter comments or a note for your reference.	
Notification	Enable this option to receive in-app notification about the status when the particular action is completed. NOTE: This option is only available when the Notification Service is deployed on the RAMP.	

Database Troubleshooting

Additional Topics:

- [Cleaning Debezium Data](#)
- [Start DBaaS Service in RAMP](#)
- [Stop DBaaS Service in RAMP](#)

Troubleshooting the Ribbon Application Management Platform (RAMP) database is covered in this section.

Cleaning Debezium Data

Use the `./cleanupDBZData.sh` script to address disk congestion issues. If Ribbon Application Management Platform (RAMP) is down for a considerable amount of time (e.g., hours), the debezium replication slot size grows (increases the `pg_wal` size at `/var/lib/pgsql/12/data/pg_wal`), which eventually increases the disk size. The presence of this large replication slot prevents RAMP from deleting the WAL logs.

Start

1. Login to RAMP as `insight`.
2. Use the following command to navigate to `/conf` folder:

```
cd /opt/sonus/ems/conf/
```

3. Run the following script to stop the kafka process, delete the connect offsets file, and drop the debezium replication slot:

```
./cleanupDBZData.sh
```

Start DBaaS Service in RAMP

Ribbon Application Management Platform (RAMP) uses PostgreSQL Database as a Service (DBaaS).

To start DBaaS service in RAMP:

1. Log on to the RAMP node as admin user.
2. Change to "postgres" user:

```
sudo -iu postgres
```

3. Start the DBaaS service:

```
dbaas_service start
```

Stop DBaaS Service in RAMP

Ribbon Application Management Platform (RAMP) uses PostgreSQL Database as a Service (DBaaS).

To stop DBaaS for troubleshooting RAMP, follow this procedure.

1. Log on to the RAMP node as the admin user.
2. Change to "postgres" user:

```
sudo -iu postgres
```

3. Stop the DBaaS service:

```
dbaas_service stop
```

Fault Manager Troubleshooting

Use this section to resolve common Fault Manager issues in Ribbon Application Management Platform (RAMP).

Issue	Solution
Check the status of the Fault Management (FM) processes	Enter the following commands as the insight user: <pre>/opt/fm/bin/fm status</pre> You can view the logs related to the FM background processes in the <code>/opt/fm/logs/</code> directory. You can view the log to Fault management UI in the <code>/opt/fm/logs/ui/</code> directory
Enable debug for FM process.	Every FM process has a <code>Log4j.xml</code> in the <code>/opt/fm/conf/<process>/</code> directory. The log level of process needs to be modified from info to debug in the process specific <code>log4j2.xml</code> for Logger name="com.rbbn".
Enable debug for FM GUI web applications	Every UI web application has a <code>Log4j.xml</code> in the <code>/opt/fm/conf/fm-ui/<ui-application-name>/</code> directory. The log level of process needs to be modified from info to debug in the process specific <code>log4j2.xml</code> for Logger name="com.rbbn".
The timestamp in the active alarms are incorrect.	The system stores timestamps in UTC and changes it to RAMP time zone before viewing. The timestamps for Ribbon devices are included in the trap information, so verify the time and time zone settings on the applicable device.

Issue	Solution
Alarms do not display for a node even though it is registered with RAMP.	• Navigate to Device Management > Node Management > Function Manager and click Discover for the appropriate device to ensure that RAMP is configured as a trap destination on the remote agent. This is necessary if you reinstall the agent after registering the node. • Ensure that the source IP address of traps from the device is registered in RAMP. The trap receiver rejects alarms originating from an IP address if the associated device is not registered with RAMP. Check <code>/opt/fm/logs/trap.log</code> to see all traps received. Search for “UnRegistered Node” text to find unknown IP addresses received.
View alarm count	To view count of active alarms, navigate to Fault Manager > Administration > Present Usage > Number of active alarm records. To view count of alarms in history, navigate to Fault Manager > Administration > Present Usage > Number of alarm history records

General Troubleshooting

This page provides information on some general issues which may occur while operating Ribbon Application Management Platform (RAMP).

Issue	Solution
The RAMP GUI does not launch after login.	Verify that you have disabled any popup blockers installed on your system. These applications interfere with the proper operation of RAMP.
RAMP is slow.	Often, the cause of excessively slow operation and response from RAMP is due to insufficient computer resources or a slow network connection. Verify the adequacy of your network connection.
“java.io.IOException: Not enough space” error message in RAMP trace log or popup message.	This error indicates that the /tmp directory on your UNIX system may have reached capacity. The tmp directory is used for many UNIX system operations and lack of space in this directory will make your system unusable. You must clean up the tmp directory.

Issue	Solution
After closing the RAMP , another user can reopen it without entering a username and password.	Use the Exit icon to close Insight. After Insight is closed verify that ALL browser windows are closed to clear cached passwords.

Issue	Solution
RAMP reboots continuously when the disk is full.	When the disk is full, all operations fail and Ribbon Application Management Platform (RAMP) reboots continuously, up to three times. To resolve this issue, free up space in the disk and perform the following procedure: 1. Log onto the RAMP as the admin user. 2. Change to the root user: <pre data-bbox="737 583 1453 667">sudo su -</pre> 3. Navigate to the following directory: <pre data-bbox="737 730 1453 814">/opt/sonus/ems/kafka/data/zookeeper/version-2</pre> 4. List the log files: <pre data-bbox="737 877 1453 961">ls -ltr</pre> Example <pre>total 460712 -rw-r-----. 1 insight insight 67108880 Aug 2 10:04 log.1 -rw-r--r--. 1 insight insight 67108880 Aug 5 01:55 log.c3 -rw-r--r--. 1 insight insight 61264 Aug 12 16:41 snapshot.1ad9e -rw-r--r--. 1 insight insight 67108880 Aug 12 16:41 log.56dc -rw-r--r--. 1 insight insight 67108880 Aug 16 04:02 log.1ada0 -rw-r--r--. 1 insight insight 67108880 Aug 16 05:06 log.249ee -rw-r--r--. 1 insight insight 67108880 Aug 17 07:25 log.24bef -rw-r--r--. 1 insight insight 67108880 Aug 20 12:24 log.27ccc -rw-r-----. 1 insight insight 67108880 Aug 20 12:28 log.30d50 -rw-r--r--. 1 insight insight 67108880 Aug 24 00:19 log.30d59</pre> 5. Delete the latest log.* file.

Issue	Solution
	Example <pre>rm log.30d59</pre>

GSX Troubleshooting

In this section:

- [GSX Navigator Troubleshooting](#)
- [GSX Upgrade Troubleshooting](#)

GSX Navigator Troubleshooting

This page provides information on GSX Navigator issues and handling solutions.

Issue	Solution
GSX Navigator slow or does not work	treeAgeOverrideMinutes is a configurable parameter in SystemConfig.txt. By default, this parameter is not set. If treeAgeOverrideMinutes is set to 0, GSX Navigator tree will be re-discovered after 60 minutes from the last discovery. Without setting this parameter in SystemConfig.txt, Nav tree will be rediscovered after 5 years from the last discovery, means the tree was accepted up to 5 years old. It can be set to any integer, for example 30, means the tree will be accepted for 30 minutes old without new discovery. For "manual" discovery type, set this parameter to 0 for the tree to update with the configuration changes from Navigator in 60 minutes after the last discovery.
No node names appear in the Node pull-down list.	Register the GSX9000 nodes first with Ribbon Application Management Platform (RAMP) before you manage the nodes with RAMP. Register the appropriate GSX9000 nodes from the Node tab in the Administration section.

Issue	Solution
What is the discovery time of the displayed Navigator Tree?	Position the mouse over the Up To Date text area located at the bottom left corner of the Node Objects window. A popup tooltip will display the date and time the last discovery took place.
The Object tree appears to be out of date with the device configuration on the GSX9000.	The displayed Object tree is usually the most recent one available on RAMP. Occasionally RAMP may not be notified of configuration changes that take place on the GSX9000 made by another user with RAMP or another management application. Click the Get button to force a new discovery of the device.
The Object tree appears to be frequently out of date with the device configuration on the GSX9000.	The displayed Object tree is usually the most recent one available on RAMP. RAMP relies on traps from the GSX9000 for notifications that the configuration of the device has been changed from another management application or telnet session.
Discovery of a GSX9000 device takes a long time.	Typical discovery of a GSX9000 device should take between 2 and 30 seconds, depending on the device configuration, on network latency and the load on RAMP.
An error message indicating a timeout is displayed when attempting to discover a GSX9000.	If the GSX9000 device cannot be reached after 30 seconds, an attempt is made by RAMP to cycle through the alternate IP Addresses for the device. If necessary, an attempt is made to register RAMP as a management client on the GSX9000 if an existing entry cannot be found. If none of the above are successful, an error message will be displayed indicating that a timeout was experienced while contacting the device. If the GSX9000 cannot be reached: • Verify the correct IP Addresses, SNMP community strings and Telnet password under the Node tab in the Administration section. • Verify that the maximum number of management clients has not been exceeded on the device. • Verify network connectivity to the device.

GSX Upgrade Troubleshooting

In this section:

- [Package Import Failures](#)
- [Software Copy Failures](#)
- [GSX Runtime Check Failures](#)
- [Firmware Upgrade Failures](#)
- [Software Upgrade Failure](#)
- [Post Upgrade Script Failures](#)
- [RAMP Failover During GSX Upgrade Process](#)

While Ribbon has endeavored to make this feature robust, the process of upgrading a GSX, either manually or automatically using this feature, is a complicated operation and may halt/fail for a variety of reasons. The following sections provide information on possible causes of failure and actions that you can take to rectify the situations.

Note

The sections that follow do not represent all possible modes of failure. In the event of failure, review the "GSX Installation and Upgrade Guide" and/or contact Ribbon Support.

From DSI v15.1 onwards, the "root" user is disabled by default. Enable the "root" user manually under `/etc/ssh/sshd_config` file, restart the service, discover the DSI with "root" credentials in the node registration page, and initiate the GSX upgrade.

Package Import Failures

As part of the package import process, Ribbon Application Management Platform (RAMP) untars the software release package and then uncompresses and untars the Install package. During this process, RAMP verifies the images contained in the Install package. The package import operation may fail due to any of the following:

- The import fails if the required space is not available in the RAMP staging directory. The minimum required space is configurable using the parameter **Local Disk Space Minimum** located in **System > Settings > Application Config**. Refer to [Application Configuration](#). To rectify this issue, free additional space in the staging directory `/opt/rbbn/ems/weblogic/sonusEms/data/gsxSwStaging` or change the minimum setting.
- The import fails, if the GSX software image is invalid. In most cases RAMP generates an error message providing information concerning the image. To rectify this issue, obtain a new software image from Ribbon.
- The import fails if the image is for an older, unsupported software image. You must upgrade to a later, supported release to use this feature. Refer to the appropriate *GSX Release Notes* and/or the *GSX Installation and Upgrade Guide* to verify your upgrade path.

Software Copy Failures

When you start an Upgrade Task, RAMP uses SCP to copy the GSX software installation packages to the associated DSI/NFS servers.

One possible failure point for the copy operation is incorrect or missing DSI/NFS passwords. If the copy operation fails, first verify that the DSI/NFS password supplied on the Node Registration page is correct.

Note

If you start multiple upgrade tasks on the GSXs in an Upgrade Job and a copy failure occurs for one or more GSX software packages, **RAMP** transitions the failed tasks to an ERROR state, but allows the other tasks to continue until achieving the GSX_UPGRADE_READY state. At this point, you can either continue operations with the non-ERROR state tasks or correct the error and restart all tasks.

If a copy operation fails and the passwords are correct, perform the following instructions:

- Examine the Audit Log for any of the error codes shown in the table below. The table also provides a mapping of the error code to issue. Use this mapping to correct the problem indicated:

Audit Log Error to Reason Mapping

Error Code	Reason
11	Failure: Malformed or out of range ipAddress
12	Failure: Installation files not copied to NFS
31	Failure: Staging dir not created on NFS
51	Failure: User dsi not setup on NFS
52	Failure: Could not untar GSX package on NFS
53	Failure: Date not current for some of the installed images on NFS
54	Failure: verify Image failed on NFS
55	Failure: Could not copy scripts to new software release directory on NFS
56	Failure: GSX software install failed
57	Failure: Could not find tar to install GSX software
58	Failure: Insufficient disk space on the NFS

Note

If you receive an Error Code 58, adjust the space required on the DSI/NFS during verification through the NFS Disk Space Minimum setting in **System > Settings > Application Config > GsxUpgrade**. For more information, refer to [Application Configuration](#).

If after examining the Audit Log, if the mode of failure is undeterminable, examine the nfsSetup.log file for error messages that might indicate the problem. This file is located either in `/global/home/gsxUpgradeStaging` or `/export/home/gsxUpgradeStaging` directory of the DSI/NFS.

After correcting the issue causing the copy failure, click **Start** to retry the software copy operation by clicking the **Start** button.

Note

If you are unable to determine the cause of the copy failure and elect to copy the files manually, perform the remaining upgrade process manually.

GSX Runtime Check Failures

The GSX runtime checks consists of three operations: a Gateway Signaling Port Status check, a GSX Protection Mode check, and a Link Status check. Each of these operations may fail. Some possible causes/remedies are:

- A failure of the Gateway Signaling Port Status check fails indicates that some gateway signaling ports are not in service. Manually return all gateway signaling port to an in service state. After remedying the issue, restart the upgrade process by clicking the **Start** button.
- If the Protection Mode check fails, one possible cause is that the GSX could not write its parameter file in the allotted time. This can occur due to a slow network connection to the DSI/NFS server. If the parameter file is not written in the allotted time, increase the value of the **PIF Write Timeout** setting in **System > Settings > Application Config > GsxUpgrade**. For more information, refer to [Application Configuration](#). After increasing this value, restart the upgrade by clicking the **Start** button.
- If the Protection Mode check fails because the GSX is not fully protected, consult the applicable *GSX Installation and Upgrade Guide* for additional information concerning protection before attempting to proceed with your upgrade. The GSX Upgrade Automation application supports upgrades only for GSXs that are fully protected.
- If the Link Status check fails, one possible cause is that the number of standby port failures exceeds the number of active port failures. It is also possible that the number of active failures exceeds the configured threshold. In either case you must correct the issue on the GSX before proceeding with the upgrade.

Firmware Upgrade Failures

If the firmware upgrade fails, you must manually correct the problem on the GSX before continuing with the upgrade. Refer to the applicable *GSX Installation and Upgrade Guide* for details regarding firmware upgrades. Once you correct the issue causing the problem, restart the upgrade by clicking **Start**.

Software Upgrade Failure

If a GSX LSWU failure occurs while the GSX is in the `SW_UPGRADE_RUNNING` state, the Upgrade Automation process does not complete the required LSWU operations. You must intervene to fix the cause of the failure and manually complete the software upgrade. After manually completing the software upgrade, return to the Automation Upgrade GUI and click **Start** to synchronize the state information on [RAMP](#) and the GSX (state =

`SW_UPGRADE_FINISHED` after the synchronization). You can then initiate any post-upgrade scripts, if required, and commit the software upgrade.

Post Upgrade Script Failures

If a post upgrade script fails, commit the software upgrade and then repair and rerun the script manually. If needed, abort the task and enter any notes required.

RAMP Failover During GSX Upgrade Process

If RAMP experiences an HA failover from the primary system to the standby while a GSX Automated Upgrade task is running, the state of the tasks as displayed on the new active system will depend upon the state prior to failover and may require user intervention to synchronize with the GSX's actual state. The following table provides details concerning the original state, state shown on the new active system and any user intervention required to continue the upgrade.

States After RAMP HA Failover

State Before Failover	State After Failover	User Action Required
UPGRADE_TASK_START	UPGRADE_TASK_CREATED	Click Start
COPYING_TO_PRI_NFS	UPGRADE_TASK_CREATED	Click Start
SW_COPIED_PRI_NFS	UPGRADE_TASK_CREATED	Click Start
COPYING_TO_SEC_NFS	UPGRADE_TASK_CREATED	Click Start
FW_VERSION_MISMATCH	FW_VERSION_MISMATCH	Click Upgrade FW
FW_UPGRADE_RUNNING	FW_VERSION_MISMATCH	Click Upgrade FW
SW_UPGRADE_READY	SW_UPGRADE_READY	Click Upgrade FW
SW_UPGRADE_RUNNING	SW_UPGRADE_READY	Click Upgrade FW
COMMIT_REQUIRED	COMMIT_REQUIRED	Click Commit
POST_UPGRADE_SCRIPT_RUNNING	COMMIT_REQUIRED	Click Commit
GSX_UPGRADE_FINISHED	GSX_UPGRADE_FINISHED	None
ABORTED	ABORTED	None
ERROR	ERROR	None

RAMP CNF Troubleshooting

In this section:

- [Identify Container Restart](#)
- [Invalid timeZone Causes a RAMP Container to Restart](#)
- [Check I/O of a RAMP Pod](#)

Use this section to troubleshoot and recover the Ribbon Access Management Platform (RAMP) Cloud Native Functionality (CNF) device.

Identify Container Restart

Identify a container that unexpectedly restarted in a specific pod:

```
oc get pods
```

check the RESTARTS column.

Example

```
[ssequira@cli-server ~]$ oc get pod
NAME                READY   STATUS    RESTARTS   AGE
sanrampsdr-rampcnf-0 2/2     Running   3          45d
[ssequira@cli-server ~]$
```

If a pod displays the restart value as non-zero, for example, `sanrampsdr-rampcnf-0`, use the command `oc describe pod <pod_name>` to check:

- which container restarted,
- reason for the container to restart,
- the container restart time, and
- to check the events.

```
[ssequira@cli-server ~]$ oc describe pod sanrampsdr-rampcnf-0
Name:                sanrampsdr-rampcnf-0
Namespace:           ems-svt
Priority:              0
Node:                worker-3.ott-ocp1.lab.rbbn.com/172.29.114.28
Start Time:          Tue, 06 Jun 2023 02:48:53 -0400
Labels:               app=sanrampsdr-rampcnf-pod
                     app.kubernetes.io/instance=sanrampsdr
                     cnf_uid=e56aa2ea-2c1e-4964-970e-b86eaff727d9
                     cnfc_uid=b3e021dc-947d-4c19-824b-3412c267509c
                     component=prometheus-rbbn-otel-agent
                     controller-revision-hash=sanrampsdr-rampcnf-6c6f765f68
                     element=rampcnf
```

```

group=sanrampsdr
ns_uuid=8aebafe4-50c2-4f52-a43f-b7d1a40df51c
servicetype=observability
statefulset.kubernetes.io/pod-name=sanrampsdr-rampcnf-0
tenant=ramp
version=23.06.00-71
Annotations: k8s.v1.cni.cncf.io/network-status:
    [{
      "name": "openshift-sdn",
      "interface": "eth0",
      "ips": [
        "10.231.31.162"
      ],
      "default": true,
      "dns": {}
    }, {
      "name": "ems-svt/ext-net-1",
      "interface": "eth1",
      "ips": [
        "172.29.115.21"
      ],
      "mac": "9e:8d:f8:e1:75:47",
      "dns": {}
    }]
k8s.v1.cni.cncf.io/networks: /ext-net-1@eth1
k8s.v1.cni.cncf.io/networks-status:
    [{
      "name": "openshift-sdn",
      "interface": "eth0",
      "ips": [
        "10.231.31.162"
      ],
      "default": true,
      "dns": {}
    }, {
      "name": "ems-svt/ext-net-1",
      "interface": "eth1",
      "ips": [
        "172.29.115.21"
      ],
      "mac": "9e:8d:f8:e1:75:47",
      "dns": {}
    }]
openshift.io/scc: privileged
prometheus.io/path: /metrics
prometheus.io/port: 9101
prometheus.io/scheme: http
prometheus.io/scrape: true
Status: Running
IP: 10.231.31.162
IPs:
  IP: 10.231.31.162
Controlled By: StatefulSet/sanrampsdr-rampcnf

```

Containers:

rbbn-rampcnf-container:

Container ID: cri-o://

8da0f1a0eb40d38a7aee80f2dd7ad7ce3ca7480c74d9d195de1e2d9089f85486

Image: artifactory1-ot.rbbn.com/ems-docker-prod-plano/production/

rampcnf/rbbn-ramp-cnf:23.06.00-71

Image ID: artifactory1-ot.rbbn.com/ems-docker-prod-plano/production/

rampcnf/rbbn-ramp-cnf@sha256:4a8fce85ab250cad96fbfbe268179932573a33f842ad4645e629cf48d2bbd783

Ports: 443/TCP, 80/TCP, 22/TCP

Host Ports: 0/TCP, 0/TCP, 0/TCP

State: Running

Started: Mon, 12 Jun 2023 05:31:24 -0400

Last State: Terminated

Reason: Error

Exit Code: 2

Started: Sun, 11 Jun 2023 13:28:27 -0400

Finished: Mon, 12 Jun 2023 05:31:21 -0400

Ready: True

Restart Count: 3

Limits:

cpu: 16

ephemeral-storage: 130Gi

memory: 64Gi

Requests:

cpu: 16

ephemeral-storage: 130Gi

memory: 64Gi

Liveness:

```
exec [/bin/sh -c su - insight -c "/opt/sonus/ems/conf/
probe_reboot.sh" >> /opt/raid/dockerEmsInit.log] delay=300s timeout=60s period=180s
#success=1 #failure=3
```

Readiness:

```
exec [/bin/sh -c state=`/opt/sonus/ems/conf/opensaf/AS/
commons.sh getGrState`; if [ $state != "standby" ]; then exit 0; else exit 1; fi >> /
opt/raid/dockerEmsInit.log] delay=30s timeout=20s period=30s #success=1 #failure=1
```

Startup:

```
exec [/bin/sh -c su - insight -c "/opt/sonus/ems/conf/
probe.sh" >> /opt/raid/dockerEmsInit.log] delay=480s timeout=20s period=10s #success=1
#failure=40
```

Environment:

TZ: Asia/Kolkata

ZONE: Asia/Kolkata

PGHOST: /tmp

PG_PRIMARY_USER: primaryuser

PG_MODE: primary

PROMETHEUS_PROBE_PORT: 10050

SC_PORT: 10050

container_type: ramp

etcdauth: NO

cert:

key:

ca:

certid: 4200

MY_CONTAINER_NAME: rbbn-rampcnf-container

MY_POD_NAME: sanrampsdr-rampcnf-0 (v1:metadata.name)

```

NODE_NAME:                (v1:spec.nodeName)
NS_UUID:                   8aebafe4-50c2-4f52-a43f-b7d1a40df51c
CNF_UUID:                  e56aa2ea-2c1e-4964-970e-b86eaff727d9
CNFC_UUID:                 b3e021dc-947d-4c19-824b-3412c267509c
LINUX_LOG_PATH:            /var/log/logcentral/
RAMP_NET_CONF_FILE:        /opt/ribbon/configmap/network/ramp_netconfig.yaml
Mounts:
  /etc/podinfo from podinfo (rw)
  /opt/raid/ from sanrampsdr-ramp-pv-storage (rw)
  /opt/rbbn/rbbn-telemetry/pm_stats/input/ from sanrampsdr-pmstats-pvc (rw)
  /opt/ribbon/configmap/fm from alarm-exporter-config (rw)
  /opt/ribbon/configmap/network from ramp-net-config (rw)
  /opt/sonus/userData from ramp-config-volume (rw,path="authKeys")
  /tmp/ from ramp-empty-dir (rw)
  /var/log/logcentral/ from ramp-logcentral-dir (rw)
  /var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-b5bdw (ro)
rbbn-telemetry-agent:
  Container ID:   cri-o://
2c6c1d8f1a89e62086ab8b941dc143d8cffda44c8347cf6531f90b401472ca50
  Image:          artifactory1-ot.rbbn.com/ribbon_telemetry-docker-prod-plano/
release/rbbn_telemetry_collector:v1.3.4
  Image ID:       artifactory1-ot.rbbn.com/ribbon_telemetry-docker-prod-plano/
release/rbbn_telemetry_collector@sha256:bb7faee7376a231cfca128f182093ed3c12b93da67ee6
39ce564ae76f5bbacad
  Port:           9101/TCP
  Host Port:      0/TCP
  State:          Running
    Started:      Tue, 06 Jun 2023 02:56:17 -0400
  Ready:          True
  Restart Count:  0
  Limits:
    cpu:          4
    memory:       8Gi
  Requests:
    cpu:          4
    memory:       8Gi
  Liveness:       exec [/bin/sh -c /opt/rbbn/rbbn-telemetry/bin/liveness_probe.sh]
delay=30s timeout=1s period=10s #success=1 #failure=5
  Readiness:      exec [cat /opt/rbbn/rbbn-telemetry/etc/.ready_probe] delay=30s
timeout=1s period=10s #success=1 #failure=5
  Environment:
    TZ:            Asia/Kolkata
    RUN_PMS:       YES
    LOG_CONF:      YES
    METRIC_CONF:   YES
    MY_NODE_NAME:  (v1:spec.nodeName)
    MY_POD_NAME:   sanrampsdr-rampcnf-0 (v1:metadata.name)
    MY_POD_NAMESPACE:  ems-svt (v1:metadata.namespace)
    MY_POD_UID:    (v1:metadata.uid)
  Mounts:
    /fluent-logs/ from sanrampsdr-rbbn-otel-agent-pvc (rw)
    /home/buf/ from fluent-buf (rw)

```

```

/opt/rbbn/rbbn-telemetry/etc/config-pm_stats.yaml from ramp-otel-config-volume
(rw,path="config-pm_stats.yaml")
/opt/rbbn/rbbn-telemetry/etc/config.yaml from ramp-otel-config-volume
(rw,path="config.yaml")
/opt/rbbn/rbbn-telemetry/etc/podinfo from obs-podinfo (rw)
/opt/rbbn/rbbn-telemetry/etc/ramp-obs-parser.conf from ramp-obs-parser-volume
(rw,path="ramp-obs-parser.conf")
/opt/rbbn/rbbn-telemetry/logs/ from telemetry-logs (rw)
/opt/rbbn/rbbn-telemetry/pm_stats/input/ from sanrampsdr-pmstats-pvc (rw)
/var/log/ from ramp-empty-dir (rw)
/var/log/logcentral/ from ramp-logcentral-dir (rw)
/var/run/secrets/kubernetes.io/serviceaccount from kube-api-access-b5bdw (ro)
Events:
Type      Reason      Age           From          Message
----      -
Normal    Pulled      111m          kubelet       Container image
"artifact2.eng.sonusnet.com/ems-docker-prod-plano/production/rampcnf/rbbn-ramp-
cnf:23.09.00-151" already present on machine
Normal    Created     111m (x2 over 19h)  kubelet       Created container rbbn-rampcnf-
container
Normal    Started     111m (x2 over 19h)  kubelet       Started container rbbn-rampcnf-
container
Warning   Unhealthy   101m (x19 over 19h) kubelet       Startup probe failed:

[ssequeira@cli-blr-1 ~]$

```

Invalid timeZone Causes a RAMP Container to Restart

The RAMP CNF container unexpectedly restarts if the timeZone value is invalid. In such a scenario, the DbaaS startup fails. Check the validity of the timeZone value that was set in the `/var/log/dbaas/dbaas_service.*.log` during the RAMP CNF deployment.

A sample output of `/var/log/dbaas/dbaas_service.10353.log`

```

waiting for server to start....2023-07-26 06:30:07.315 GMT [30750] LOG:  invalid value
for parameter "TimeZone": "IST"
2023-07-26 06:30:07.315 GMT [30750] LOG:  invalid value for parameter "log_timezone":
"IST"
2023-07-26 06:30:07.315 GMT 172.29.115.220 [30750 start=2023-07-26 06:30:07 GMT]: u=[]
db=[] app=[] c=[] s=[64c0bd6f.781e:3] tx=[:0]FATAL:  configuration file "/var/lib/pgsql/
13/data/postgresql.auto.conf" contains errors
stopped waiting
pg_ctl: could not start server
Examine the log output.

```

Check the validity of the timeZone value that was set during the RAMP CNF deployment.

Example of an invalid timezone

```
[hasingh@cli-blr-1 rbbn-ramp-cnf]$ helm get values hasingh | grep timeZone
timeZone: IST
```

Set the timeZone to one of the values in the "TZ identifier" column in the list of timezones at: https://en.wikipedia.org/wiki/List_of_tz_database_time_zones.

Example

```
[ssequeira@cli-blr-1 rbbn-ramp-cnf]$ helm get values sanrampblr4 | grep timeZone
timeZone: Asia/Kolkata
```

Check I/O of a RAMP Pod

If RAMP CNF is restarting, check the I/O speed. To check the I/O of RAMP CNF, login to the RAMP CNF container and execute `/opt/sonus/ems/conf/benchmark.sh`. This command provides the disk write performance (seconds) of ephemeral and persistent volume. Recommended values for ephemeral disk is less than 2 and persistent volume is less than 50.

```
-bash-4.4$ /opt/sonus/ems/conf/benchmark.sh
```

Reference output from 16vcpu 64GB RAMP CNF on Ribbon OCP cluster ,working dir /opt/rbbn/ems

```
#####
CPU: SHA256-hashing 500 MB
    2.605 seconds
CPU: gzip-compressing 500 MB
    2.931 seconds
CPU: AES-encrypting 500 MB
    0.826 seconds
```

Reference disk write performance(seconds) in the /opt/raid directory.

```
VMware                               Avg. 14.445
Openstack HP SAN cinder               Avg. 24.4039
Azur STANDARD SSD LRS                 Avg. 64.988
Azur PREMIUM SSD LRS                 Avg. 44.5847
HP DL380p Gen 8 Local HDD:           Avg. 0.9702
IBM V3700 FC-attached RAID:           Avg. 13.2959
HP MSA 204 iSCSI-attached SAN:        Avg. 22.8417
#####
```

```
Running Tests.....
```

```
Testing CPU speed
```

```
CPU: SHA256-hashing 500 MB
```

```
3.168 seconds
```

```
CPU: gzip-compressing 500 MB
```

```
3.528 seconds
```

```
CPU: AES-encrypting 500 MB
```

```
1.103 seconds
```

```
#####
```

```
Testing ephemeral storage write performance
```

```
Testing sequential write speed(seconds) on file /opt/sonus/ems/testIO.out
```

```
Results: 20.054 21.621 19.780 20.850 19.492 19.782 21.070 19.882 19.228
19.730
```

```
Min: 19.228 Max: 21.621 Avg: 20.1489
```

```
#####
```

```
Testing external volume write performance
```

```
Testing sequential write speed(seconds) on file /opt/raid/testIO.out
```

```
Results: 31.351 33.090 33.153 32.402 32.204 34.963 35.922 36.142 35.483
32.729
```

```
Min: 31.351 Max: 36.142 Avg: 33.7439
```

```
-bash-4.4$
```

RAMP GR Auto-Switchover Troubleshooting

In this section:

- [etcd RAMP Interactions](#)
- [RAMP GR when One etcd is Down](#)
 - [Check etcd Health on etcd](#)
 - [Check etcd Health Using RAMP](#)
- [RAMP GR when Multiple etcds are Down](#)
 - [Check etcd Health on etcd](#)
 - [Check etcd Health Using RAMP](#)
 - [RAMP Recovery Procedure](#)

Use this section to troubleshoot and recover from a RAMP GR automatic switchover after an etcd outage.

Three etcd VMs are required to monitor a Ribbon Application Management Platform (RAMP) Geographically Redundant (GR) deployment for automatic switchover. For information on how the etcd VMs are involved in the GR deployment, refer to [Configuring RAMP GR with Automatic Switchover Enabled](#).

In a typical GR deployment, RAMP instances are deployed at two separate geographic sites. To enable automatic switchover, a VM running etcd is deployed at each RAMP site and at a third, “neutral” site. Together, the three etcd instances are responsible for determining which RAMP instance is active.

etcd RAMP Interactions

The etcd is a key value store deployed as a quorum of three nodes. This makes the etcd highly available when one of the nodes is down. The RAMP maintains etcd as a marker for high availability to mark its current node. The RAMP sets itself active by adding its node identifier as a value to a unique set of keys in etcd.

Below are the set of keys:

Use the lock key to determine if the current node is Active. Most actions are performed on the key to set the node values (SC-1 and SC-3) while relocating or processing the kill failure. SC-1 refers to the configured Active instance, and SC-3 is the Standby instance:

```
/opensaf_<clustername>_<epoch>/opensaf_consensus_lock
```

The `opensaf_write_test` is a test key is only set when a new node tries to monitor etcd (in case of a reboot scenario):

```
/opensaf_<clustername>_<epoch>/opensaf_write_test
```

Perform the following steps to get the value from etcd for a specific key:

Start

1. Check current key and values on etcd using the following procedure:
 - a. Log on to etcd as `sysadm` user.
 - b. Switch to `root` user.

```
sudo su -
```

- c. Log on to the etcd pod:

```
podman exec -it etcd-pod-etcd bash
```

- d. Get the value for a specific key:

```
etcdctl get <Key>
```

Example output:

```
etcd@dndetcd1:/opt/bitnami/etcd$ etcdctl get /opensaf_emscluster_1724546650/
opensaf_consensus_lock
/opensaf_emscluster_1724546650/opensaf_consensus_lock SC-1
```

2. Check the current key and values on RAMP:

- a. Log on to the RAMP as an `admin` user.
- b. Switch to `root` user.
- c. Run the `osaf-utils` command:

```
/opt/opensaf/osaf-utils
```

- d. Select option 5 in the Menu to retrieve the value from `etcd`.

Note

The Opensaf Consensus interacts with the etcd quorum. The interactions between RAMP and etcd can be found in the log file located at `/var/log/opensaf/etcd.log`. RAMP uses a cron job to monitor the reachability of etcd nodes on both the active and standby RAMP instances. If connectivity between these nodes is lost, an alarm is triggered through user insight.

Example output:

```
[2024-08-08 15:16:54 root@rakeshgr02: /opt/sonus/ems/conf/opensaf ]# ./osaf-utils
```

```
~~~~~
```

```
-- MENU
```

```
~~~~~
```

- 1) DISPLAY: OpenSAF Controller Status
- 2) DISPLAY: OpenSAF Process Monitor Status
- 3) DISPLAY: Insight SG status
- 4) DISPLAY: etcd Server Health
- 5) DISPLAY: osaf key value from etcd
- 6) DISPLAY: ALL etcd keynames
- 7) SWACT: OpenSAF Controller
- 8) SWACT: OpenSAF Process Monitor
- 9) ALIGN Process Monitor with OpenSAF Controller

10) RESET Process Monitor SUs

0) Exit

Please enter your choice: 5

- Retrieving current key value from etcd...
- etcd result: /opensaf_emsclusterrakk_1722230877/opensaf_consensus_lock: 'SC-3'

etcd Alarms

RAMP 1 State	RAMP2 State	N/w b/w RAMP1 & RAMP2	etcd Quorum	RAMP1 to etcd Quorum	RAMP2 to etcd Quorum	Effect
Active	Standby	YES	YES	YES	YES	In Service.
Active	Standby	YES	YES	YES	YES	In Service. No switchover as the ETCD quorum is available, 1/3 of ETCD nodes are reachable, and the ETCD quorum is available.
Active	Standby	YES	YES	YES	NO	In Service. No Switchover/failover.
Active	Standby	YES	YES	NO	YES	Active RAMP - reboot after 10 minutes of connection lost between RAMP and ETCD. Standby Node - becomes Active.
Active	Standby	YES	NO	NO	NO	Continuous reboots between Active and Standby, As the Active node cannot be established because all the etcds are down.
Active	Standby	NO	YES	YES	YES	Active node - In Service. State of Standby - node down, Standby goes for reboot.

RAMP 1 State	RAMP2 State	N/w b/w RAMP1 & RAMP2	etcd Quorum	RAMP1 to etcd Quorum	RAMP2 to etcd Quorum	Effect
Active	Standby	NO	YES	YES	NO	Active node - In Service. State of Standby - node down Standby goes for reboot.
Active	Standby	NO	YES	NO	YES	Active Node - reboot after 10 minutes of connection lost b/w ramp and etcd. Standby Node - becomes Active.

Refer to the [RAMP Release Notes](#) for the ETCD version(s) tested with RAMP.

When the ETCD Quorum is lost and does not recover, the RAMP reboot occurs. To stop this scenario, when the ETCD quorum fails, keep the current active node intact until the ETCD can be recovered. The current behavior of ETCD is as follows:

Scenario	RAMP 1 State	RAMP 2 State	N/w b/w RAMP1 & RAMP2	Etcd Quorum	RAMP1 to etcd Quorum	RAMP2 to etcd Quorum	Effect	Fix
RAMP Active connection fail with etcd Quorum	Active	Standby	YES	YES	NO	YES	Active RAMP - reboot after 10 minutes of connection lost between the RAMP and the etcd. Standby Node - becomes Active.	Active will remain active unless it breaks cause of other issues. after that changes will not affect the flow. Standby - remains in Standby.

Quorum Fails	Active	Standby	YES	NO	NO	NO	Continuous Reboots between Active and Standby as Active Node cannot be established, this will happen until <code>opensaf</code> limit is reached, which is 5.	Active will remain active unless it breaks cause of other issues. after that changes will not affect the flow. Standby - will remain on standby.

RAMP GR when One etcd is Down

There is no impact on the RAMP GR if one etcd is down. Recover the etcd and check the etcd cluster status.

Check etcd Health on etcd

Use this procedure to check the etcd health on the etcd:

Start

1. Log on to one of the etcd VMs as a `root` user.
2. Check the cluster state:

```
root@services3 ~]# /etc/rbbn/appservices/scripts/etcdStatus.py
```

Example

```
root@services3 ~]# /etc/rbbn/appservices/scripts/etcdStatus.py
+-----+-----+-----+-----+-----+
| Name | ID | Endpoint | Leader | Healthy |
+-----+-----+-----+-----+-----+
| services1 | 64386b664d63723b | http://10.52.23.94:2379 | false | true |
| services2 | 81dcb39d0b4f7142 | http://10.52.23.249:2379 | true | true |
| services3 | c88e907d0579400a | http://10.52.22.115:2379 | false | true |
+-----+-----+-----+-----+-----+
```

Check etcd Health Using RAMP

Use this procedure to health-check the etcd through RAMP:

Start

1. Log on to the RAMP as a `root` user
2. Connect etcd to the RAMP:

```
# /opt/opensaf/osaf-utils
```

Example

```
# /opt/opensaf/osaf-utils

~~~~~
-- MENU
~~~~~

1) DISPLAY: OpenSAF Controller Status
2) DISPLAY: OpenSAF Process Monitor Status
3) DISPLAY: Insight SG status

4) DISPLAY: etcd Server Health
5) DISPLAY: osaf key value from etcd
6) DISPLAY: ALL etcd keynames

7) SWACT: OpenSAF Controller
8) SWACT: OpenSAF Process Monitor

9) ALIGN Process Monitor with OpenSAF Controller
10) RESET Process Monitor SUS

0) Exit
Please enter your choice:
```

3. Enter **4** to check etcd server health.

Example

```
- Checking etcd health - OSAF_ENDPOINTS:
'10.52.23.94:2379,10.52.23.249:2379,10.52.22.115:2379'
10.52.22.115:2379 is healthy: successfully committed proposal: took = 3.891546ms
10.52.23.249:2379 is healthy: successfully committed proposal: took = 4.620617ms
10.52.23.94:2379 is healthy: successfully committed proposal: took = 5.579312ms
```

RAMP GR when Multiple etcds are Down

The RAMP stops working if multiple etcds are down. In such scenarios, you must check to ensure network connectivity and that the etcds are shut down. Check the etcd status after the etcds are recovered and the etcd VM are up and running.

Check etcd Health on etcd

Use this procedure to check the etcd health on the etcd:

Start

1. Log on to one of the etcd VMs as a `root` user.
2. Check the cluster state:


```
root@services3 ~]# /etc/rbbn/appservices/scripts/etcdStatus.py
```

Example

```
root@services3 ~]# /etc/rbbn/appservices/scripts/etcdStatus.py
```

Name	ID	Endpoint	Leader	Healthy
services1	64386b664d63723b	http://10.52.23.94:2379	false	true
services2	81dcb39d0b4f7142	http://10.52.23.249:2379	true	true
services3	c88e907d0579400a	http://10.52.22.115:2379	false	true

Check etcd Health Using RAMP

Use this procedure to health-check the etcd through RAMP:

Start

- 1. Log on to the RAMP as a root user.
- 2. Connect etcd to RAMP:

```
# /opt/opensaf/osaf-utils
```

Example

```
# /opt/opensaf/osaf-utils

-- MENU

1) DISPLAY: OpenSAF Controller Status
2) DISPLAY: OpenSAF Process Monitor Status
3) DISPLAY: Insight SG status

4) DISPLAY: etcd Server Health
5) DISPLAY: osaf key value from etcd
6) DISPLAY: ALL etcd keynames

7) SWACT: OpenSAF Controller
8) SWACT: OpenSAF Process Monitor

9) ALIGN Process Monitor with OpenSAF Controller
10) RESET Process Monitor SUs
```

```
0) Exit
Please enter your choice:
```

3. Enter **4** to check etcd server health.

Example

```
- Checking etcd health - OSAF_ENDPOINTS:
'10.52.23.94:2379,10.52.23.249:2379,10.52.22.115:2379'
10.52.22.115:2379 is healthy: successfully committed proposal: took = 3.891546ms
10.52.23.249:2379 is healthy: successfully committed proposal: took = 4.620617ms
10.52.23.94:2379 is healthy: successfully committed proposal: took = 5.579312ms
```

RAMP Recovery Procedure

The `opensaf` process stops running if the etcd is down for over two hours. Use this procedure to recover RAMP:

Start

1. Log on to the active RAMP as an `admin` user.
2. Change to `root` user:

```
# sudo su -
```

3. Start the `opensafd` process:

```
# systemctl start opensafd
```

4. Check `opensafd` process status. It should be running:

```
# systemctl status opensafd
```

5. Ensure that the RAMP related processes are running. For more information, refer to [Check RAMP Status](#).
6. Log on to the standby RAMP as an `admin` user.
7. Change to `root` user:

```
# sudo su -
```

8. Start the `opensafd` process:

```
# systemctl start opensafd
```

9. Ensure the `opensafd` process is up and running:

```
# systemctl status opensafd
```

10. Ensure that the RAMP-related processes are running. For more information, refer to [Check RAMP Status](#).

Note

- If any process fails, you can disable/enable the health check of the particular process using `manage0saf.sh` script. For more information, refer to [Retrieve System Information](#).
- The `/opt/sonus/ems/gr_standby` file is applicable only if the auto failover mode is disabled on RAMP. The `gr_standby` should not be created in the auto failover enabled RAMP.

The alarms `sonusHARACArbitratorDownNotification` and `sonusHARACArbitratorUpNotification` are raised if the `etcd` is down. For more information on alarms, refer to:

- [sonusHARACArbitratorDownNotification](#)
- [sonusHARACArbitratorUpNotification](#)

Retrieve System Information

In this section:

- [View RAMP Log Files](#)
- [Analyze System Performance](#)
- [Debug OpenSAF](#)

If Ribbon Global Product Support (GPS) personnel ask you to retrieve certain log files or information from your Ribbon Application Management Platform (RAMP) device to assist in diagnosing an issue, use the following steps to gather and forward the details.

View RAMP Log Files

To generate log files for debugging:

1. Access RAMP as the insight user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the insight user.
2. Generate a tar file containing log and configuration files associated with RAMP:

```
/opt/sonus/ems/conf/archiveLogs.sh
```

3. When prompted to enter comments, type a description or a reason for creating the log file. The following is an example:

```
Following upgrade operation.
```

4. Press ENTER to move to the next line.
5. Enter a period (.) and press ENTER to conclude your comments and to save the logs.
The script shows status messages as it creates the file.

The log files are stored as a single tar.gz file at `/opt/sonus/ems` in the format `logFiles-<RAMP host name>-<timestamp>.tar.gz`

Analyze System Performance

If you experience problems with RAMP performance, GPS can request that you run a utility to gather system performance data.

To run the performance analysis utility:

1. Access RAMP as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the root user.
2. Check the RAMP performance settings and statistics:

```
/etc/sonus/analyzeSystem.sh
```

RAMP displays performance settings and statistics related to the following:

- RAMP installation
 - System configuration
 - CPU configuration
 - Memory configuration
 - TMPFS (Temp File System) usage
 - Process information
 - Memory map for RAMP process
 - Postgres processes
 - Postgres process shared memory
 - Other processes
 - Shared memory stats
 - Disk usage
 - TCP protocol statistics
 - UDP protocol statistics
 - TCP driver configuration
 - Network interface configuration
 - ETCD Arbitrators Health for GR systems which has auto-switchover enabled
3. You can run following command for additional information:

```
/etc/sonus/analyzeSystem.sh -health
```

Some of the key performance metrics displayed as a result of this command are:

Metrics	Summary
Output of <code>/opt/sonus/ems/emsMgmt status</code>	◦ EMS instantiated version. ◦ Status of each process. ◦ HA Mode ◦ Configured and Current states. ◦ of EMS HA Nodes. ◦ Hostnames of HA/GR peers. ◦ IP addresses of HA/GR peers. ◦ SBCAPI deployment location.
Output of <code>/etc/sonus/RDSyncStatus</code>	◦ Replication Status on current node ◦ Log sequence number and any lag between primary and standby ◦ Sync status
Host Information	◦ Hostname ◦ Kernel Version ◦ Uptime ◦ Last Reboot Time ◦ OS Architecture ◦ Current System Date & Time
Disk Usage	◦ Currently Mounted File System ◦ Disk Usage on all mounted file system ◦ Health status on each mounted disk usage
IO Stats	The following are captured from 3 samples with a 3 second delay: ◦ Average CPU Util % based on idle % ◦ Average IO WAIT % ◦ Average Steal Time %
Inode Usage	◦ Inode usage ◦ Inode usage percentage ◦ Health status on each inode usage
CPU Usage	◦ All core utilization ◦ Utilization Summary ◦ Overall load average
Netstat Report	◦ Packets In ◦ Packets Out ◦ Packets Dropped ◦ MTU ◦ Overall Health by pkts drop

Metrics	Summary
ETCD Arbitrators	Health for all ETCD Arbitrators configured for GR systems which has auto-switchover enabled.
Top 10 Process Analysis	Top 10 CPU/MEM processes

Debug OpenSAF

If directed by GPS to make changes to OpenSAF on your device, RAMP provides a utility for this purpose.

To run the OpenSAF utility:

- 1. Access RAMP as the root user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the root user.
- 2. View OpenSAF commands:

```
/opt/sonus/ems/conf/manage0saf.sh
```

Sample output:

```
# /opt/sonus/ems/conf/manage0saf.sh

*****
*****
***
*** 1.  Disable OpenSAF (disables the link) ***
*** 2.  Disable & Stop OpenSAF             ***
*** 3.  Enable OpenSAF                     ***
*** 4.  Start OpenSAF                      ***
*** 5.  EMS Status Check                   ***
*** 6.  OpenSAF status check                ***
*** 7.  Stop EMS(w/o OpenSAF)              ***
*** 8.  Start EMS(w/o OpenSAF)             ***
*** 9.  Healthcheck disable                ***
*** 10. Healthcheck enable                 ***
*** 11. Healthcheck Modify                 ***
*** 12. FM/PM/LM/ACS Service Enable        ***
*** 13. FM/PM/LM/ACS Service Disable      ***
***                                       ***
*** 0.  Exit                               ***
*****
*****

Which action do you want to perform :
```

- 3. Enter the number for the option requested by GPS.
The output from the utility depends on the chosen option. Continue to work with GPS on the next steps to take.

Tools Troubleshooting

This page provides information on Tools issues on Ribbon Application Management Platform (RAMP) and handling solutions.

Issue	Solution
I am not receiving Call Trace information. I only receive error messages.	Check the Call Trace error log file. <code><BASE_DIR>/weblogic/callTraceSlave/ctslave.log.err</code>
What do I do if the user gets “ERROR:INTERNAL:NFS server(s) may not be configured properly. Inform System Administrator to consult error logs.”	Check the Call Trace error log file. <code><BASE_DIR>/weblogic/callTraceSlave/ctslave.log.err</code>
Error “server is busy processing another request.”	By default, only two users are allowed to use the Call History tool simultaneously due to the excessive load it creates on RAMP. This error means that two other RAMP users are using the Call History tool and you should wait a few seconds before trying again.
Create Report dialog remains blank for about 30 seconds after coming up.	This means that the primary or the secondary NFS is down and the Call History tool is timing out while trying to automount the file systems. The dialog should be populated with information after the timeout period.
It takes a long time for the CDRs to get displayed after inputting filters and clicking OK in the Create Report dialog.	If the filters are too broad, then a large number of CDRs need to be formatted and displayed on the HTML page, which could take a while. Try providing narrower filters which will return less number of records.
Trunk Group Rename > Failure to rename the trunk group on the PSX.	Verify that the PSX is properly configured on the GSX and RAMP. Verify that the trunk group you are renaming exists on the PSX and is associated with the GSX gateway. If the renaming operation failed due to a primary/replica replication failure, consult the PSX documentation set for information concerning recovery from primary/replica replication failures

RAMP will not start if it cannot establish a connection to its Database Instance. Any one of a number of problems can prevent RAMP from establishing a connection to the database.

These problems include:

- Configuration Errors.
- One of the required database processes are not running.

Unlock or Recover a User Account for Sysadmin or Any Admin User

This procedure is intended for VMware, KVM, RHEV, and OpenStack sysadmin or admin users to unlock their accounts when the password has expired or they exceeded the number of password attempts.

Perform the following procedure to recover a locked admin or sysadmin user.

Note

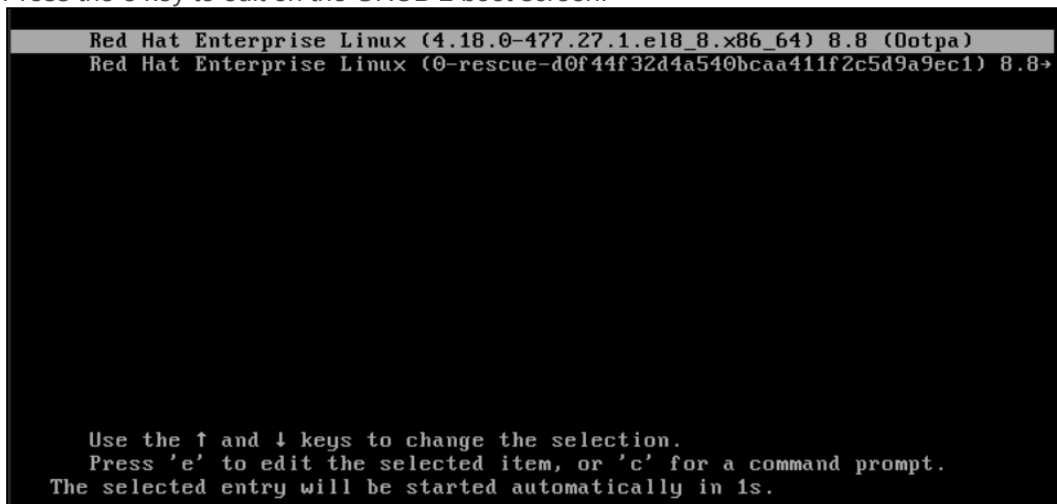
Use IDRAC virtual console or an equivalent remote access controller virtual console to get the grub menu for ROHOS host OS user recovery

The grub parameters in grub menu entry may vary from Host OS to Guest OS.

This procedure is applicable for all supported platforms like VMware, KVM, RHEV, and OpenStack platforms.

Start

1. Log on to the cockpit of the KVM hypervisor or an equivalent Virtual Machine (VM) manager for different hypervisors.
2. Select the required VM.
3. Open the serial console and reset or reboot the Virtual machine.
4. Press the **e** key to edit on the GRUB 2 boot screen:



```
Red Hat Enterprise Linux (4.18.0-477.27.1.el8_8.x86_64) 8.8 (0otpa)
Red Hat Enterprise Linux (0-rescue-d0f44f32d4a540bcaa411f2c5d9a9ec1) 8.8→

Use the ↑ and ↓ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
The selected entry will be started automatically in 1s.
```

5. Provide the GRUB root credentials using the default username as `root` and the default password as `shipped`. For the ROHOS host default grub credentials, the username as `root` and the password as `ribbon`.

6. Delete the highlighted text in the following screen:

```
load_video
set gfx_payload=keep
insmod gzio
linux ($root)/vmlinuz-4.18.0-477.27.1.el8_8.x86_64 root=/dev/mapper/vg00-root \
ro console=tty0 splash=silent showopts intel_iommu=on iommu=pt nmi_watchdog=0 \
rd.live ram rd.lvm.lv=vg00/root biosdevname=0 net.ifnames=0 console=tty0 console=ttyS0 crashkernel=auto NOHZ=OFF pti=on audit=1 audit_backlog_limit=8192 ipv6.disable=0 fips=1 boot=UUID=28515e7c-6388-425c-80a6-627a186463a6 page_poison=1 vsyscall=none slub_debug=P
initrd ($root)/initramfs-4.18.0-477.27.1.el8_8.x86_64.img $tuned_initrd

Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
discard edits and return to the menu. Pressing Tab lists
possible completions.
```

7. Add the following parameters at the end of the Linux command.

```
rd.break
rd.lvm.lv=vg00/var_log
```

```
load_video
set gfx_payload=keep
insmod gzio
linux ($root)/vmlinuz-4.18.0-477.27.1.el8_8.x86_64 root=/dev/mapper/vg00-root \
ro console=tty0 splash=silent showopts intel_iommu=on iommu=pt nmi_watchdog=0 \
rd.live ram rd.lvm.lv=vg00/root rd.lvm.lv=vg00/var_log biosdevname=0 net.ifnames=0 crashkernel=auto NOHZ=OFF pti=on audit=1 audit_backlog_limit=8192 ipv6.disable=0 fips=1 boot=UUID=28515e7c-6388-425c-80a6-627a186463a6 page_poison=1 vsyscall=none slub_debug=P rd.break
initrd ($root)/initramfs-4.18.0-477.27.1.el8_8.x86_64.img $tuned_initrd

Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
discard edits and return to the menu. Pressing Tab lists
possible completions.
```

8. When the system is ready, press **Ctrl+x** to boot the system with the changed parameters.
9. If the file system is read-only and is mounted on `/sysroot/`. Mount the `var_log lvm` since faillock tally directory exist on `/var/log/`. Remount the file system as writable and Enter chroot system:

```
switch_root:/# mount -o remount,rw /sysroot
switch_root:/# mkdir -p /sysroot/var/log/
switch_root:/# mount /dev/vg00/var_log /sysroot/var/log/
switch_root:/# chroot /sysroot
```

10. To unlock:
- A specific user:

```
faillock --reset --user <USERNAME>
```

- b. A sysadmin user

Example

```
faillock --reset --user sysadm
```

- c. All locked users:

```
faillock --reset
```

11. Force the file-system relabeling:

```
touch /.autorelabel
```

12. Use the `exit` command to exit the `chroot` system.

13. Unmount the logical volume:

```
#umount /sysroot/var/log
```

14. Run the reboot command to reboot the server.

Wait for the file-system relabeling to complete. Depending on your system speed and number of files this might take some time. Be patient.

15. Log on after the system reboots.

Administration Guide

In this section:

- [Accessing RAMP VNF Using Active Directory](#)
 - [Reconfiguring Active Directory](#)
- [Accessing RAMP CNF Using Active Directory](#)
 - [Custom Host and DNS Configuration for Kubernetes Pods](#)
- [Daily Maintenance Activities](#)
- [How to Start and Stop RAMP](#)
- [How to Start and Stop Sonus Agent](#)
- [How to Rediscover the localhost](#)
- [How to Control the Network Range](#)
- [How to Prepare RAMP for ROHOS Upgrade](#)
- [Access RAMP Database](#)
- [Attach RAMP to Multiple Disjointed IP Networks](#)
 - [Using RAMP as a PSX Proxy](#)
 - [Separation of OAM and Signaling Networks on Call Trace in RAMP](#)
- [Backup and Restore](#)
 - [Take a Backup of RAMP for Daily Maintenance](#)
 - [Take a Backup of RAMP for Upgrade](#)
 - [Restore from Backup on RAMP Standalone](#)
 - [Restore from Backup on RAMP GR](#)
 - [Restore a Master Key File](#)
 - [Restore a Master Key File \(.KF\) Manually](#)
- [Check Software Versions](#)
 - [Check RAMP Version](#)
 - [Check LINTEL Platform Version in RAMP](#)
 - [Check Red Hat Enterprise Linux Server Version in RAMP](#)
 - [Check PostgreSQL Version in RAMP](#)
 - [Check Java Version in RAMP](#)
 - [Check DBaaS Version in RAMP](#)
 - [Check Platform Kernel Version in RAMP](#)
- [Check Status](#)
 - [Check RAMP Status](#)
 - [Check Deployment Status of Services in RAMP](#)
- [Change Time Zone on RAMP](#)
- [Deploy Optional Services on RAMP](#)
- [Download Files from Ribbon Support Portal](#)
- [Export the RAMP Configuration Tables](#)
- [Install PSX Manager on RAMP](#)
- [Managing Accounts and Passwords](#)
 - [Manage RAMP Account Names and Passwords](#)
 - [Manage User Accounts](#)
 - [Establish Passwordless Connection from an External Server to RAMP](#)
 - [Establish RAMP CNF Active-Standby Instance Passwordless Connection](#)
 - [Change the GRUB Password](#)
- [Managing Log Files](#)
 - [Change Log Level](#)
 - [Configure Silent Auth for Jboss CLI](#)

- RAMP Log Files
- Reset Admin Password for Jboss CLI
- Managing the NTP Server
 - Add Multiple NTP Servers for RAMP
 - Synchronize RAMP with the NTP Server
- Managing Redundancy
 - Check Database and File Replication Status
 - Change the Role of a Node in RAMP GR
 - Reconfigure a Standby Node in RAMP GR
 - Tear Down RAMP GR
 - Replace a Node in RAMP GR
- Managing Resources
 - Manage Resources for RAMP on KVM
 - Manage Resources for RAMP on OpenStack
 - Manage Resources for RAMP on VMware ESXi
- Managing Secure Communications
 - Secure Login to the RAMP GUI
 - Secure Communication Between RAMP and Devices
 - Enable Key-Based Authentication for SSH
- Manually Generate Traps and Verify Alarm Handling
- Proxy Manager
- Legacy Device Management

This guide is intended for users with RAMP administrator privileges to perform administrative tasks required to manage Ribbon Application Management Platform (RAMP).

Accessing RAMP VNF Using Active Directory

The Ribbon Application Management Platform (RAMP) allows user authentication through an active directory. The default authentication mechanism on Linux systems is through the local system database: `/etc/passwd` and `/etc/shadow`. All the systems, applications, and operational users are authenticated using the local database. This process is extended by using Microsoft Active Directory or any other equivalent tool if your Linux system is registered with such an active directory domain.

Using the procedure on this page, configure the Linux system to register in the Active Directory domain and enable extending user authentication to be performed from the Active Directory Domain Controller (ADDC). Then, active directory users are allowed access to the Linux system.

SAMBA and Winbind are used to add the Linux system to the active directory and for user authentication.

Prerequisites

To register a linux system to the ADDC and centralized authentication:

- The Windows Server is installed.
- Networks are configured in the Windows Server, including Internet Protocol (IP), Netmask, and Gateway.
- ADDC is installed on the Windows Server.
- The Domain Name Server (DNS) is configured in the Windows Server, DNS pointing to the active directory server (if DNS is hosted in the domain controller).
- The Windows Server is configured as the domain controller.
- The domain name for ADDC is set.
- The clock is synchronized between the Linux system and the active directory server.

- You are able to reach (ping) the Linux system from the Windows Server.
- Create operational users from the active directory. Only these users are authenticated through the active directory.
- Provide passwords to the active directory users while adding them.

The procedure to configure the Linux system is based on the example values provided in this table for the active directory server. Replace all these example values according to your active directory and Linux parameters.

Parameters with Example Values

Parameter	Example Value
Active Directory Domain name	sonusqa.net
Domain Netbios name	sonusqa
Windows Server computer name	PSXAD2019
Short Domain name	testdom
Windows Server admin user name	administrator
Linux Hostname	cmpsource

Note

The procedure is based on Windows server 2012 R2 active directory server.

Note

You are allowed to provide a Hostname for the Linux system up to 15 characters. For more information, refer to <https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/naming-conventions-for-computer-domain-site-ou>.

Configure the Linux System

Perform this procedure to register the Linux system to the active directory domain on the Linux system:

Start

1. Log on to the Linux system as `root` user.
2. To ensure the RPM Package Managers (RPM) are installed, use the command:

Example:

```
rpm -qa | grep samba
```

Example output:

```
samba-ldb-ldap-modules
samba-common-libs
samba-winbind-clients
samba-common
samba-client-libs
samba-winbind
samba-client
samba-libs
samba-dcerpc
samba-winbind-modules
samba
samba-common-tools
```

3. Ensure the Windows active directory server IP address is reachable (ping) from the Linux system:

```
ping <Windows Server IP>
```

4. Create a backup directory to store all the files that may change as part of this procedure:

```
mkdir backup
```

5. Backup the files to the newly created `backup` directory:

```
cp --parents -p /etc/hosts backup
cp --parents -p /etc/resolv.conf backup
cp --parents -p /etc/samba/smb.conf backup
cp --parents -p /etc/nsswitch.conf backup
cp --parents -p /etc/pam.d/fingerprint-auth backup
cp --parents -p /etc/pam.d/smartcard-auth backup
cp --parents -p /etc/pam.d/password-auth backup
cp --parents -p /etc/pam.d/system-auth backup
```

6. To ensure the Linux system resolves the hostname for the ADCC, configure the `/etc/hosts` file:

```
127.0.0.1      "linux-hostname"."Active Directory Domain name" "linux-hostname"
host_IP "linux-hostname"."Active Directory Domain name" "linux-hostname"
```

```
Windows server IP    "Windows Server computer name" "Windows Server computer
name"."Active Directory Domain name" "Domain netbios name" "Domain netbios name
in caps" "Active Directory Domain name"
```

Verify the file: `/etc/hosts` :

Note

The names are provided based on the Example Values table. Replace all these example values according to your active directory and Linux parameters.

```
127.0.0.1    localhost
::1         localhost
127.0.0.1    localhost.localdomain
172.19.52.153 cmpsource cmpsource.localdomain
10.54.48.246 PSXAD2019 PSXAD2019.sonusqa.net sonusqa SONUSQA sonusqa.net
```

7. Verify the IP address of the active directory in the `/etc/resolve.conf` file:

Note

Ribbon recommends adding the name server details to the heat template while creating the instance.

For KVM/VMware deployments, do this through the `configdrive.iso` file.

```
nameserver <IP address of the Windows Active Directory server>
```

Example:

```
nameserver 10.54.48.246
```

8. Provide the Windows Server name to ensure it is reachable (ping) and the DNS is resolved:

```
ping "<Windows Server name>". "<Active Directory Domain name>"
```

The ping and name resolution must be successful.

Note

The server time offset should be minimal or zero. If it is not zero, ensure the clock time in the Windows Server is correct, the Network Time Protocol (NTP) server is up and running, and the time zone is configured accurately in the Linux host.

Ensure the `chronyd.service` is running.

Ensure the NTP is in the synchronized state. To synchronize, refer to [Synchronize RAMP with the NTP Server](#).

9. Configure the active directory domain name, realm, and User Identification (UID) mapping in the SAMBA configuration file: `/etc/samba/smb.conf` based on the following table:

Active Directory Configuration Parameters

Parameter	Default Value	Description
Workgroup		The domain Netbios name. The workgroup for the client, You can specify the <code>Netbios</code> name of the domain or a short domain name.
realm		Active Directory Domain name. The domain the client is a part-of. Provide the full domain name.
client user spnego	Yes	To enable Simple and Protected NEGOTiation.
winbind enum users	Yes	If the <code>winbind enum</code> users parameter is No , the calls to the <code>getpwent</code> system call does not return any data. If set to Yes , the " <code>getent passwd</code> " query lists all the users (including the active directory users).
winbind enum groups	Yes	To return all groups (including the active directory group) when queried using " <code>getent group</code> ".
winbind use default domain	No	If set to No (recommended), always specify the active directory users along with the domain name. For example, " <code>DOMAIN_NAME+ADusername</code> ".

Parameter	Default Value	Description
winbind separator	+	Separator for winbind between the DOMAIN_NAME and the AD_USERNAME . For example, " DOMAIN_NAME+ADusername "
idmap config * : backend	tdb	The mapping mechanism between the User id (UID) and the Test DB (tdb) is Test DB. It enables to allocate the user IDs of the new active directory users.
idmap config * : range		The UID range allocated to the active directory users. In Lintel systems, the UID range for users is specified in the file: /etc/login.defs . Adjust the range according to your preference: Non lintel systems: 1500-2000 Lintel systems: 1000-60000
template shell	/bin/bash	Specifies the shell to allocate for a new user: /bin/bash

To configure, replace the workgroup and realm to suit your environment and run:

```
cat >/etc/samba/smb.conf
```

Example:

```
cat >/etc/samba/smb.conf << EOF
[global]
workgroup = SONUSQA
realm = SONUSQA.NET
netbios name = SANRAMPTest
security = ADS
client use spnego = yes
server signing = auto
server string = Samba Server
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = no
winbind separator = +

idmap config * : backend = tdb
```

```
idmap config * : range = 1500-2000

template shell = /bin/bash
EOF
```

10. Update the `krb5.conf` with the active directory domain name:

Example output:

```
# cat /etc/krb5.conf
# To opt out of the system crypto-policies configuration of krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will not be recreated.
includedir /etc/krb5.conf.d/

[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
#    default_realm = EXAMPLE.COM
    default_ccache_name = KEYRING:persistent:%{uid}
    default_realm = SONUSQA.NET
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
SONUSQA.NET = {
    kdc = PSXAD2019.sonusqa.net
    admin_server = PSXAD2019.sonusqa.net
}

[domain_realm]
.sonusqa.net = SONUSQA.NET
sonusqa.net = SONUSQA.NET
```

11. Join the domain, for example: sonusqa.net from the Linux system:

Note

To join the Linux system to the active directory domain, you must know the Windows Server user name and password with administrative privileges. For example in this instance: The user name is "administrator" and the password is "administrator".

Example:

```
net ads join -S "<Windows Server computer name>".<Active Directory Domain name>"  
-U administrator
```

The system prompts you to provide the password:

Example:

```
net ads join -S PSXAD2019.sonusqa.net -U Administrator
```

Note

This is an expected warning and can be ignored:
DNS update failed: NT_STATUS_UNSUCCESSFUL

12. To verify the success of the `net ads join -S "<Windows Server computer name>"` command:

```
net ads testjoin
```

Example output:

```
Join is OK
```

13. Ensure that the Name Service Switch (NSS) configuration file: `/etc/authselect/user-nsswitch.conf` is having an entry pointing to `winbind` for password, group, and shadow database. Edit and add `winbind` database for password, group, and shadow. Ensure the file: `/etc/authselect/user-nsswitch.conf` is having these entries.
- a. Copy the `/etc/nsswitch.conf` file to `/etc/authselect/user-nsswitch.conf`:

```
yes | cp /etc/nsswitch.conf /etc/authselect/user-nsswitch.conf  
cp: overwrite '/etc/authselect/user-nsswitch.conf'?
```

- b. Append `winbind` details in `/etc/authselect/user-nsswitch.conf`:

```
passwd:    files winbind  
shadow:    files winbind  
group:     files winbind
```

Here the order of the database in the file is important, because it directs the system to first go for local authentication, if it fails then tries `winbind` authentication from the active directory.

14. Recheck to ensure all the information is correct:

```
net ads info
```

Example output:

```
# net ads info
LDAP server: 10.54.48.246
LDAP server name: PSXAD2019.SONUSQA.NET
Realm: SONUSQA.NET
Bind Path: dc=SONUSQA,dc=NET
LDAP port: 389
Server time: Mon, 25 Nov 2024 20:27:38 IST
KDC server: 10.54.48.246
Server time offset: 712
Last machine account password change: Mon, 25 Nov 2024 19:56:04 IST
```

15. Start and enable the `winbind` service:

```
systemctl enable winbind
systemctl start winbind
systemctl status winbind
```

Example output:

```
# systemctl enable winbind
Created symlink /etc/systemd/system/multi-user.target.wants/winbind.service → /usr/lib/systemd/system/winbind.service.
# systemctl start winbind
# systemctl status winbind
• winbind.service - Samba Winbind Daemon
   Loaded: loaded (/usr/lib/systemd/system/winbind.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2024-11-25 20:16:20 IST; 1s ago
     Docs: man:winbindd(8)
           man:samba(7)
           man:smb.conf(5)
  Main PID: 148616 (winbindd)
    Status: "winbindd: ready to serve connections..."
     Tasks: 5 (limit: 408593)
    Memory: 14.2M
    CGroup: /system.slice/winbind.service
            └─148616 /usr/sbin/winbindd --foreground --no-process-group
```

```

└─148618 /usr/sbin/winbindd --foreground --no-process-group
└─148619 /usr/sbin/winbindd --foreground --no-process-group
└─148621 /usr/libexec/samba/samba-dcerpcd --libexec-rpcds --ready-
signal-fd=23 --np-helper --debuglevel=0
└─148630 /usr/libexec/samba/rpcd_lsad --configfile=/etc/samba/smb.conf
--worker-group=4 --worker-index=5 --debugl>

Nov 25 20:16:20 cmpsource winbindd[148616]: [2024/11/25 20:16:20.608322, 0] ../../
/source3/winbindd/winbindd.c:1443(main)
Nov 25 20:16:20 cmpsource winbindd[148616]: winbindd version 4.19.4 started.
Nov 25 20:16:20 cmpsource winbindd[148616]: Copyright Andrew Tridgell and the
Samba Team 1992-2023
Nov 25 20:16:20 cmpsource systemd[1]: Started Samba Winbind Daemon.
Nov 25 20:16:20 cmpsource samba-dcerpcd[148621]: [2024/11/25 20:16:20.669289, 0]
../../source3/rpc_server/rpc_host.c:2846(m>
Nov 25 20:16:20 cmpsource samba-dcerpcd[148621]: samba-dcerpcd version 4.19.4
started.
Nov 25 20:16:20 cmpsource samba-dcerpcd[148621]: Copyright Andrew Tridgell and
the Samba Team 1992-2023
Nov 25 20:16:20 cmpsource rpcd_lsad[148630]: [2024/11/25 20:16:20.801545, 0] ../../
./source3/rpc_server/rpc_worker.c:1130(rpc>
Nov 25 20:16:20 cmpsource rpcd_lsad[148630]: rpcd_lsad version 4.19.4 started.
Nov 25 20:16:20 cmpsource rpcd_lsad[148630]: Copyright Andrew Tridgell and the
Samba Team 1992-2023

```

16. Verify if the the system is able to access the active directory:

- a. Check if the trust secret through RPC calls succeeded:

```
wbinfo -t
```

Example output:

```
checking the trust secret for domain SONUSQA via RPC calls succeeded
```

- b. List the active directory groups:

```
wbinfo -g
```

Example output:

```

SONUSQA+domain computers
SONUSQA+domain controllers
SONUSQA+schema admins
SONUSQA+enterprise admins
SONUSQA+cert publishers
SONUSQA+domain admins
SONUSQA+domain users

```

```

SONUSQA+domain guests
SONUSQA+group policy creator owners
SONUSQA+ras and ias servers
SONUSQA+allowed rodc password replication group
SONUSQA+denied rodc password replication group
SONUSQA+read-only domain controllers
SONUSQA+enterprise read-only domain controllers
SONUSQA+cloneable domain controllers
SONUSQA+protected users
SONUSQA+key admins
SONUSQA+enterprise key admins
SONUSQA+dnsadmins
SONUSQA+dnsupdateproxy

```

17. To create a user's home directory if it does not already exist when an active directory user logs on to the RAMP, append, `session required pam_mkhomedir.so skel=/etc/skel/ umask=002` in the file: `/etc/pam.d/password-auth` :

```
cat /etc/pam.d/password-auth
```

Example output:

```

# Generated by authselect on Tue Nov 26 05:01:30 2024
# Do not modify this file manually.

auth      required                                pam_env.so
auth      required                                pam_faildelay.so
delay=2000000
auth      sufficient                              pam_unix.so nullok
auth      [default=1 ignore=ignore success=ok]    pam_usertype.so isregular
auth      sufficient                              pam_winbind.so
use_first_pass
auth      required                                pam_deny.so

account   required                                pam_unix.so broken_shadow
account   sufficient                              pam_localuser.so
account   sufficient                              pam_usertype.so issystem
account   [default=bad success=ok user_unknown=ignore] pam_winbind.so
account   required                                pam_permit.so

password  requisite                              pam_pwquality.so
local_users_only
password  sufficient                              pam_unix.so sha512 shadow
nullok use_authok
password  sufficient                              pam_winbind.so
use_authok
password  required                                pam_deny.so

```

```

session      optional      pam_keyinit.so revoke
session      required      pam_limits.so
-session     optional      pam_systemd.so
session      optional      pam_oddjob_mkhomedir.so
session      [success=1 default=ignore] pam_succeed_if.so service
in crond quiet use_uid
session      required      pam_unix.so
session      optional      pam_winbind.so
session      required      pam_mkhomedir.so skel=/
etc/skel/ umask=002

```

18. If the line, `AllowUsers` exists in the file: `/etc/ssh/sshd_config` comment it. Additionally, set `UseDNS` as `no` and `ChallengeResponseAuthentication` as `no` in the same file. Restart the SSH daemon to apply the changes: and restart the `sshd`.

For example:

Before commenting:

```
AllowUsers admin postgres insight guouser
```

After commenting:

```
#AllowUsers admin postgres insight guouser
```

- a. Update `UseDNS` and `ChallengeResponseAuthentication` in `/etc/ssh/sshd_config`:

```
UseDNS no

ChallengeResponseAuthentication no
```

- b. Restart `sshd`:

```
systemctl restart sshd
```

- c. Check the status of `sshd`:

```
systemctl status sshd
```

Example output:

```

sshd.service - OpenSSH server daemon
  Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor
 preset: enabled)
  Active: active (running) since Mon 2024-11-25 20:34:10 IST; 8s ago
    Docs: man:sshd(8)
          man:sshd_config(5)

```

```

Main PID: 204508 (sshd)
  Tasks: 1 (limit: 408593)
  Memory: 1.1M
  CGroup: /system.slice/sshd.service
          └─204508 /usr/sbin/sshd -D -oCiphers=aes256-ctr,aes128-gcm@openssh.c
om,aes128-ctr -oMACs=hmacc-sha2-512,hmacc-sha2->

Nov 25 20:34:10 cmpsource systemd[1]: Starting OpenSSH server daemon...
Nov 25 20:34:10 cmpsource sshd[204508]: Server listening on 0.0.0.0 port 22.
Nov 25 20:34:10 cmpsource sshd[204508]: Server listening on :: port 22.
Nov 25 20:34:10 cmpsource systemd[1]: Started OpenSSH server daemon.

```

19. To provide a sudo privilege for a specific active directory user, at the end of the `/etc/sudoers` file, include the following:

```
<Domain Netbios name>+<ADuser_name> ALL=(ALL) ALL
```

20. To provide a sudo privilege for all the users of an active directory group, at the end of the `/etc/sudoers` file, include the following:

```
%ActiveDirectoryUserGroup ALL=(ALL:ALL) ALL
```

Example output:

```
%SONUSQA+domain\ users ALL=(ALL:ALL) ALL

%Linux\ Admins ALL=(ALL:ALL) NOPASSWD:ALL
```

Where, "SONUSQA+domain\ users" and "Linux Admins" are group names in the active directory.

21. To provide `su` privileges to an active directory user, comment the following lines in the file: `/etc/pam.d/su`.

```
auth          sufficient      pam_wheel.so trust use_uid
auth          required        pam_wheel.so  use_uid
```

22. Copy the active directory configurations to the file: `/opt/raid` :

```
cp -pr /opt/rbbn/ems/conf/docker/activedirectory/ /opt/raid/
```

Example output:

```
#cp -pr /opt/rbbn/ems/conf/docker/activedirectory/ /opt/raid/
```



```

[2024-11-13 08:38:20 root@cmpsource: /opt/raid ]# cd /opt/raid/
[2024-11-13 08:38:25 root@cmpsource: /opt/raid ]# ls -ltr
total 132
drwxrwxr-x.  2 insight  insight  4096 Nov  9 19:37 activedirectory
-rwx-----.  1 insight  insight  2835 Nov  9 19:37 InsightCert.cert
-rwx-----.  1 insight  insight  3413 Nov  9 19:37 InsightCertKey.pem
drwxr-xr-x.  4 insight  insight  4096 Nov  9 19:40 pmconf
drwxr-xr-x. 16 insight  insight  4096 Nov  9 19:41 fmconf
drwxr-xr-x.  5 root     root     4096 Nov  9 23:00 devMgmt
drwxr-x---.  3 insight  insight  4096 Nov  9 23:00 sonusEms
drwx-----.  4 postgres postgres 4096 Nov  9 23:00 pgdata
drwxr-x---.  2 insight  insight  4096 Nov  9 23:00 inventoryReports
drwxr-x---.  4 insight  insight  4096 Nov  9 23:00 lnp
drwxr-x---.  4 insight  insight  4096 Nov  9 23:00 lm
drwxr-x---.  2 postgres postgres 4096 Nov  9 23:00 CA
drwxr-x---.  4 insight  insight  4096 Nov  9 23:00 auth
drwxr-xr-x.  2 insight  insight  4096 Nov  9 23:00 image_upload
-rw-r--r--.  1 root     root        0 Nov  9 23:00 databaseVersion.properties
-rw-r--r--.  1 insight  insight    258 Nov  9 23:00 sonus.conf
drwxr-x---.  5 insight  insight  4096 Nov  9 23:01 configuration
drwxr-x---.  2 insight  insight  4096 Nov  9 23:01 secure
drwxr-x---.  3 insight  insight  4096 Nov  9 23:08 dump
drwxr-x---.  4 insight  insight  4096 Nov  9 23:09 kafka
drwxr-x---.  4 root     root     4096 Nov 10 12:20 actiondb
drwxr-x---.  3 root     root     4096 Nov 10 12:20 acs
drwxr-x---.  2 insight  insight  4096 Nov 10 12:21 pyevservice
drwxr-x---.  3 root     root     4096 Nov 10 12:21 ev
drwxr-x---.  4 root     root     4096 Nov 10 12:22 evdb
drwxrwxrwx.  3 root     root     4096 Nov 10 12:24 ozone
-rw-rw----.  1 insight  insight  8836 Nov 10 12:24 iptables_rules
-rw-rw----.  1 insight  insight  1218 Nov 10 12:24 ip6tables_rules
drwxr-x---.  4 root     root     4096 Nov 10 12:24 objectstoredb
drwxr-x---.  3 root     root     4096 Nov 10 12:24 oss
-rw-r--r--.  1 insight  insight   189 Nov 13 08:17 hosts
drwxr-xr-x.  6 insight  insight  4096 Nov 13 08:38 pmdata
[2024-11-13 08:38:27 root@cmpsource: /opt/raid ]#

```

23. Change your directory to: `/opt/raid/activedirectory`:

```
cd /opt/raid/activedirectory
```

24. Create a directory `files` in the directory: `/opt/raid/activedirectory`:

```
mkdir files
```

25. Change the owner details to `insight`:

```
chown insight:insight files
```

Example output:

```
[2024-11-13 08:38:27 root@cmpsource: /opt/raid ]# cd /opt/raid/activedirectory
[2024-11-13 08:41:38 root@cmpsource: /opt/raid/activedirectory ]# mkdir files
[2024-11-13 08:42:05 root@cmpsource: /opt/raid/activedirectory ]# chown
insight:insight files
[2024-11-13 08:43:14 root@cmpsource: /opt/raid/activedirectory ]# ls -ltr
total 20
-rwxrwxr-x. 1 insight insight 3969 Nov  9 18:55 activedirectory.yaml
-rwxrwxr-x. 1 insight insight 3341 Nov  9 18:55 activedirectoryConfiguration.sh
-rwxrwxr-x. 1 insight insight  484 Nov 13 08:39 activedirectoryConfig.yml
-rw-r-----. 1 root      root    2559 Nov 13 08:39 activedirectory.log
drwxr-x---. 2 insight insight 4096 Nov 13 08:42 files
```

26. Update the password in the file: `/opt/raid/activedirectory/activedirectoryConfig.yml` :

Update password and domain in `/opt/raid/activedirectory/activedirectoryConfig.yml`

Example output:

```
cat /opt/raid/activedirectory/activedirectoryConfig.yml
files_to_move:
- src: activedirectory/files/smb.conf
  dest: /etc/samba/smb.conf
- src: activedirectory/files/krb5.conf
  dest: /etc/krb5.conf
- src: activedirectory/files/nsswitch.conf
  dest: /etc/authselect/user-nsswitch.conf
- src: activedirectory/files/password-auth
  dest: /etc/pam.d/password-auth
- src: activedirectory/files/sshd_config
  dest: /etc/ssh/sshd_config
- src: activedirectory/files/sudoers
  dest: /etc/sudoers
password: U29udXNAMTIz
domain: PSXAD2019.sonusqa.net
```

27. Backup the current active directory configurations to the directory `/opt/raid/` . These backed up configurations are used to retain the configurations after a RAMP upgrade:

`/opt/raid/activedirectory/activedirectoryConfiguration.sh -a`

Example output:

```
[2024-11-13 08:44:20 root@cmpsource: /opt/raid/activedirectory ]# /opt/raid/
activedirectory/activedirectoryConfiguration.sh -a
[2024-11-13 08:44:42 root@cmpsource: /opt/raid/activedirectory ]#
[2024-11-13 08:45:16 root@cmpsource: /opt/raid/activedirectory ]# ls -ltr files/
total 24
-rw-r-----. 1 root root  385 Nov 13 08:19 smb.conf
-rw-r-----. 1 root root 5458 Nov 13 08:20 sshd_config
-rw-r-----. 1 root root  891 Nov 13 08:21 krb5.conf
-rw-r-----. 1 root root 1845 Nov 13 08:26 password-auth
-rw-r-----. 1 root root 2976 Nov 13 08:26 nsswitch.conf
[2024-11-13 08:45:26 root@cmpsource: /opt/raid/activedirectory ]#
```

28. Enable `winbind` authentication and creation of user's home directory:

```
authselect select --force winbind with-mkhomedir
```

Example output:

```
# authselect select --force winbind with-mkhomedir
Backup stored at /var/lib/authselect/backups/2024-11-24-03-56-12.H1FwMi
Profile "winbind" was selected.
The following nsswitch maps are overwritten by the profile:
- passwd
- group

Make sure that winbind service is configured and enabled. See winbind
documentation for more information.

- with-mkhomedir is selected, make sure pam_oddjob_mkhomedir module
  is present and oddjobd service is enabled and active
- systemctl enable --now oddjobd.service
```

29. To enable and start the `oddjobd` service immediately:

```
systemctl enable --now oddjobd.service
```

Example output:

```
# systemctl enable --now oddjobd.service
```

```
Created symlink /etc/systemd/system/multi-user.target.wants/oddjobd.service → /usr/lib/systemd/system/oddjobd.service.
```

30. Apply the changes:

```
authselect apply-changes
```

Example output:

```
authselect apply-changes

Changes were successfully applied.
```

31. List of bus services before restarting `dbus` :

```
busctl | grep ^: | awk '{ print $6 }' | sort -u | tee /tmp/before
```

Example output:

```
# busctl | grep ^: | awk '{ print $6 }' | sort -u | tee /tmp/before
init.scope
NetworkManager.service
oddjobd.service
polkit.service
session-134.scope
systemd-logind.service
timedatex.service
user@0.service
user@1001.service
user@2056.service
```

32. Restart the `dbus` service:

```
systemctl restart dbus
```

33. List the bus services after restarting `dbus` :

```
busctl | grep ^: | awk '{ print $6 }' | sort -u | tee /tmp/after
```

Example output:

```
# busctl | grep ^: | awk '{ print $6 }' | sort -u | tee /tmp/after
crond.service
init.scope
oddjobd.service
opensafed.service
polkit.service
session-134.scope
timedatex.service
```

34. Identify and restart services that are in before but not in `after`, using `join` to compare the two lists:

```
systemctl restart $(join -v 1 /tmp/before /tmp/after)
```

35. Verify the RAMP `ssh` login using active directory. Refer to [Authenticating an Active Directory User](#)

Reconfiguring Active Directory

Use this procedure to reconfigure the active directory on the Ribbon Application Management Platform (RAMP).

Start

1. Configure the active directory:

```
/opt/raid/activedirectory/activedirectoryConfiguration.sh all
```

Example output:

```
/opt/raid/activedirectory/activedirectoryConfiguration.sh all
```

2. Verify the RAMP `ssh` login using active directory. Refer to, [Authenticating an Active Directory User](#).

Authenticating an Active Directory User

Use this procedure to log on to the Ribbon Application Management Platform (RAMP) using `ssh` with an active directory username.

Start

1. Test if the authentication for an active directory user is successful using the loopback address (127.0.0.1):

```
ssh DOMAIN_NAME+ADuser_name@127.0.0.1
```

When prompted, provide a valid password for a successful login:

```
DOMAIN_NAME+ADaduser_name@127.0.0.1's password:
```

Example output:

```
# ssh SONUSQA+sanjays@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:RoUCVv27wGhkyWoqWPm30tGMj/d40Q6xi0emj+nABYw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
SONUSQA+sanjays@127.0.0.1's password:
*****
** The RAMP Successfully Started                **
*****
** Version info use this command:                **
** rpm -q SONSems                               **
*****
** This file is called /etc/motd                  **
*****
Last login: Mon Nov 25 20:38:27 2024 from 127.0.0.1
OS      : Red Hat Enterprise Linux 8.10 (Ootpa)
Kernel  : 4.18.0-553.27.1.el8_10.x86_64
Ribbon  : 8.10.102-187

[2024-11-25 20:38:27 SONUSQA+sanjays@cmpsource: ~ ]#
```

2. Test for successful authentication of an active directory user with the RAMP IP address:

```
ssh DOMAIN_NAME+ADuser_name@<RAMP IP Address>
```

When prompted, provide a valid password for a successful login:

```
ssh DOMAIN_NAME+ADuser_name@<RAMP IP Address>
```

Example output:

```
ssh SONUSQA+sanjays@172.19.52.153
Warning: Permanently added '172.19.52.153' (ECDSA) to the list of known hosts.
SONUSQA+sanjays@172.19.52.153's password:
X11 forwarding request failed on channel 0
```

```

*****
** The RAMP Successfully Started          **
*****
** Version info use this command:        **
** rpm -q SONSems                        **
*****
** This file is called /etc/motd          **
*****
Last login: Mon Nov 25 20:37:25 2024 from 10.70.57.153
OS      : Red Hat Enterprise Linux 8.10 (Ootpa)
Kernel  : 4.18.0-553.27.1.el8_10.x86_64
Ribbon  : 8.10.102-187

[2024-11-25 20:37:27 SONUSQA+sanjays@cmpsource: ~ ]#

```

Accessing RAMP CNF Using Active Directory

The Ribbon Application Management Platform (RAMP) allows user authentication through an active directory. The default authentication mechanism on Linux systems is through the local system database: `/etc/passwd` and `/etc/shadow`. All the systems, applications, and operational users are authenticated using the local database. This process is extended by using Microsoft Active Directory or any other equivalent tool if your Linux system is registered with such an active directory domain.

Using the procedure on this page, configure the Linux system to register in the Active Directory domain and enable extending user authentication to be performed from the Active Directory Domain Controller (ADDC). Then, active directory users are allowed access to the Linux system.

SAMBA and Winbind are used to add the Linux system to the active directory and for user authentication.

Prerequisites

To register a linux system to the ADDC and centralized authentication:

- The Windows Server is installed.
- Networks are configured in the Windows Server, including Internet Protocol (IP), Netmask, and Gateway.
- ADDC is installed on the Windows Server.
- The Domain Name Server (DNS) is configured in the Windows Server, DNS pointing to the active directory server (if DNS is hosted in the domain controller).
- The Windows Server is configured as the domain controller.
- The domain name for ADDC is set.
- The clock is synchronized between the Linux system and the active directory server.
- You are able to reach (ping) the Linux system from the Windows Server.
- Create operational users from the active directory. Only these users are authenticated through the active directory.
- Provide passwords to the active directory users while adding them.

The procedure to configure the Linux system is based on the example values provided in this table for the active directory server. Replace all these example values according to your active directory and Linux parameters.

Parameters with Example Values

Parameters	Example Value
Active Directory Domain name	sonusqa.net
Domain Netbios name	sonusqa
Windows Server computer name	PSXAD2019
Short Domain name	testdom
Windows Server admin user name	administrator
Linux Hostname	cmpsource

Note

The procedure is based on Windows server 2012 R2 active directory server.

Note

You are allowed to provide a Hostname for the Linux system up to 15 characters. For more information, refer to <https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/naming-conventions-for-computer-domain-site-ou>.

Configure the Linux System

Perform this procedure to register the Linux system to the active directory domain on the Linux system:

Start

1. Log on to the RAMP container using the command `oc exec :`

```
oc exec -it <pod_name> -n <namespace> -- /bin/bash
```

2. To ensure the RPM Package Managers (RPM) are installed, use the command:

Example:

```
rpm -qa | grep samba
```


Example output:

```
samba-ldb-ldap-modules
samba-common-libs
samba-winbind-clients
samba-common
samba-client-libs
samba-winbind
samba-client
samba-libs
samba-dcerpc
samba-winbind-modules
samba
samba-common-tools
```

3. Ensure the Windows active directory server IP address is reachable (ping) from the Linux system:

```
ping <Windows Server IP>
```

4. Create a backup directory to store all the files that may change as part of this procedure:

```
mkdir backup
```

5. Backup the files to the newly created `backup` directory:

```
cp --parents -p /etc/hosts backup
cp --parents -p /etc/resolv.conf backup
cp --parents -p /etc/samba/smb.conf backup
cp --parents -p /etc/nsswitch.conf backup
cp --parents -p /etc/pam.d/fingerprint-auth backup
cp --parents -p /etc/pam.d/smartcard-auth backup
cp --parents -p /etc/pam.d/password-auth backup
cp --parents -p /etc/pam.d/system-auth backup
```

6. To add the active directory server details in the RAMP host file and DNS file, refer to [Custom Host and DNS Configuration for Kubernetes Pods](#).
7. To ensure the Linux system resolves the hostname for the ADCC, configure the `/etc/hosts` file:

```
127.0.0.1      "linux-hostname"."Active Directory Domain name" "linux-hostname"
host_IP "linux-hostname"."Active Directory Domain name" "linux-hostname"
Windows server IP "Windows Server computer name" "Windows Server computer
name"."Active Directory Domain name" "Domain netbios name" "Domain netbios name
in caps" "Active Directory Domain name"
```

Verify the file: `/etc/hosts` :

Note

The names are provided based on the Example Values table. Replace all these example values according to your active directory and Linux parameters.

```
127.0.0.1    localhost
::1         localhost
127.0.0.1    localhost.localdomain
172.19.52.153 cmpsource cmpsource.localdomain
10.54.48.246 PSXAD2019 PSXAD2019.sonusqa.net sonusqa SONUSQA sonusqa.net
```

8. Verify the IP address of the active directory in the `/etc/resolve.conf` file:

```
nameserver <IP address of the Windows Active Directory server>
```

Example:

```
nameserver 10.54.48.246
```

9. Provide the Windows Server name to ensure it is reachable (ping) and the DNS is resolved:

```
ping "<Windows Server name>". "<Active Directory Domain name>"
```

The ping and name resolution must be successful.

The server time offset should be minimal or zero. If it is not zero, ensure the clock time in the Windows Server is correct, the Network Time Protocol (NTP) server is up and running, and the time zone is configured accurately in the Linux host.

Ensure the `chronyd.service` is running.

Ensure the NTP is in the synchronized state. To synchronize, refer to [Synchronize RAMP with the NTP Server](#).

10. Configure the active directory domain name, realm, and User Identification (UID) mapping in the SAMBA configuration file: `/etc/samba/smb.conf` based on the following table:

Active Directory Configuration Parameters

Parameter	Default Value	Description
Workgroup		The domain Netbios name. The workgroup for the client, You can specify the <code>Netbios</code> name of the domain or a short domain name.
realm		Active Directory Domain name. The domain the client is a part-of. Provide the full domain name.
client user spnego	Yes	To enable Simple and Protected NEGOTiation.
winbind enum users	Yes	If the <code>winbind enum</code> users parameter is No , the calls to the <code>getpwent</code> system call does not return any data. If set to Yes , the " <code>getent passwd</code> " query lists all the users (including the active directory users).
winbind enum groups	Yes	To return all groups (including the active directory group) when queried using " <code>getent group</code> ".
winbind use default domain	No	If set to No (recommended), always specify the active directory users along with the domain name. For example, " <code>DOMAIN_NAME+ADusername</code> ".
winbind separator	+	Separator for <code>winbind</code> between the <code>DOMAIN_NAME</code> and the <code>AD_USERNAME</code> . For example, " <code>DOMAIN_NAME+ADusername</code> "
idmap config * : backend	tdb	The mapping mechanism between the User id (UID) and the Test DB (tdb) is Test DB. It enables to allocate the user IDs of the new active directory users.

Parameter	Default Value	Description
idmap config * : range		The UID range allocated to the active directory users. In Lintel systems, the UID range for users is specified in the file: <code>/etc/login.defs</code>. Adjust the range according to your preference: Non lintel systems: 1500-2000 Lintel systems: 1000-60000
template shell	/bin/bash	Specifies the shell to allocate for a new user: <code>/bin/bash</code>

To configure, replace the workgroup and realm to suit your environment and run:

```
cat >/etc/samba/smb.conf
```

Example:

```
cat >/etc/samba/smb.conf << EOF
[global]
  unix charset = UTF-8
  dos charset = ASCII
  workgroup = SONUSQA
  realm = SONUSQA.NET
  netbios name = SANRAMPTest
  security = ADS
  client use spnego = yes
  server signing = auto
  server string = Samba Server
  winbind enum users = yes
  winbind enum groups = yes
  winbind use default domain = no
  winbind separator = +

  idmap config * : backend = tdb
  idmap config * : range = 1500-2000

  template shell = /bin/bash
EOF
```

11. Update the `krb5.conf` with the active directory domain name:

Example output:

```
# cat /etc/krb5.conf
# To opt out of the system crypto-policies configuration of krb5, remove the
# symlink at /etc/krb5.conf.d/crypto-policies which will not be recreated.
includedir /etc/krb5.conf.d/

[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
#    default_realm = EXAMPLE.COM
    default_ccache_name = KEYRING:persistent:%{uid}
    default_realm = SONUSQA.NET
    dns_lookup_realm = false
    dns_lookup_kdc = true

[realms]
SONUSQA.NET = {
    kdc = PSXAD2019.sonusqa.net
    admin_server = PSXAD2019.sonusqa.net
}

[domain_realm]
.sonusqa.net = SONUSQA.NET
sonusqa.net = SONUSQA.NET
```

12. Join the domain, for example: sonusqa.net from the Linux system:

Note

To join the Linux system to the active directory domain, you must know the Windows Server user name and password with administrative privileges. For example in this instance: The user name is "administrator" and the password is "administrator".

Example:

```
net ads join -S "<Windows Server computer name>". "<Active Directory Domain name>"
-U administrator
```

The system prompts you to provide the password:

Example:

```
net ads join -S PSXAD2019.sonusqa.net -U Administrator
```

Note

This is an expected warning and can be ignored:
DNS update failed: NT_STATUS_UNSUCCESSFUL

13. To verify the success of the `net ads join -S "<Windows Server computer name>` command:

```
net ads testjoin
```

Example output:

```
Join is OK
```

14. Ensure that the Name Service Switch (NSS) configuration file: `/etc/authselect/user-nsswitch.conf` is having an entry pointing to `winbind` for password, group, and shadow database. Edit and add `winbind` database for password, group, and shadow. Ensure the file: `/etc/authselect/user-nsswitch.conf` is having these entries.

- a. Copy the `/etc/nsswitch.conf` file to `/etc/authselect/user-nsswitch.conf`:

```
yes | cp /etc/nsswitch.conf /etc/authselect/user-nsswitch.conf  
cp: overwrite '/etc/authselect/user-nsswitch.conf'?
```

- b. Append `winbind` details in `/etc/authselect/user-nsswitch.conf`:

```
passwd:    files winbind  
shadow:    files winbind  
group:     files winbind
```

Here the order of the database in the file is important, because it directs the system to first go for local authentication, if it fails then tries `winbind` authentication from the active directory.

15. Recheck to ensure all the information is correct:

```
net ads info
```

Example output:

```
# net ads info
LDAP server: 10.54.48.246
LDAP server name: PSXAD2019.SONUSQA.NET
Realm: SONUSQA.NET
Bind Path: dc=SONUSQA,dc=NET
LDAP port: 389
Server time: Mon, 25 Nov 2024 20:27:38 IST
KDC server: 10.54.48.246
Server time offset: 712
Last machine account password change: Mon, 25 Nov 2024 19:56:04 IST
```

16. Start and enable the `winbind` service:

```
systemctl enable winbind
systemctl start winbind
systemctl status winbind
```

Example output:

```
# systemctl enable winbind
# systemctl start winbind
# systemctl status winbind

winbind.service - Samba Winbind Daemon

    Loaded: loaded (/usr/lib/systemd/system/winbind.service, enabled)

    Active: active (running)

#
```

17. Verify if the the system is able to access the active directory:
- a. Check if the trust secret through RPC calls succeeded:

```
wbinfo -t
```

Example output:

```
checking the trust secret for domain SONUSQA via RPC calls succeeded
```

- b. List the active directory groups:

```
wbinfo -g
```

Example output:

```
SONUSQA+domain computers
SONUSQA+domain controllers
SONUSQA+schema admins
SONUSQA+enterprise admins
SONUSQA+cert publishers
SONUSQA+domain admins
SONUSQA+domain users
SONUSQA+domain guests
SONUSQA+group policy creator owners
SONUSQA+ras and ias servers
SONUSQA+allowed rodc password replication group
SONUSQA+denied rodc password replication group
SONUSQA+read-only domain controllers
SONUSQA+enterprise read-only domain controllers
SONUSQA+cloneable domain controllers
SONUSQA+protected users
SONUSQA+key admins
SONUSQA+enterprise key admins
SONUSQA+dnsadmins
SONUSQA+dnsupdateproxy
```

18. To create a user's home directory if it does not already exist when an active directory user logs on to the RAMP, append, `session required pam_mkhomedir.so skel=/etc/skel/ umask=002` in the file: `/etc/pam.d/password-auth` :

```
cat /etc/pam.d/password-auth
```

Example output:

```
# cat /etc/pam.d/password-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authselect is run.
auth      required      pam_env.so
auth      sufficient    pam_unix.so try_first_pass nullok
auth      required      pam_deny.so

account   required      pam_unix.so
```



```

password    requisite    pam_pwquality.so try_first_pass local_users_only retry=3
authtok_type=
password    sufficient   pam_unix.so try_first_pass use_authok nullok sha512
shadow
password    required      pam_deny.so

session     optional     pam_keyinit.so revoke
session     required     pam_limits.so
#-session   optional     pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet
use_uid
session     required     pam_unix.so
session     required     pam_mkhomedir.so skel=/etc/skel/ umask=002

```

19. If the line, `AllowUsers` exists in the file: `/etc/ssh/sshd_config` comment it. Additionally, set `UseDNS` as `no` and `ChallengeResponseAuthentication` as `no` in the same file. Restart the SSH daemon to apply the changes: and restart the `sshd`.

For example:

Before commenting:

```
AllowUsers admin postgres insight guouser
```

After commenting:

```
#AllowUsers admin postgres insight guouser
```

- a. Update `UseDNS` and `ChallengeResponseAuthentication` in `/etc/ssh/sshd_config`:

```
UseDNS no

ChallengeResponseAuthentication no
```

- b. Restart `sshd`:

```
ps -eaf | grep sshd | grep -v grep | awk '{print $2}' | xargs kill -9
```

- c. Check the status of `sshd`:

```
ps -ef | grep sshd
```

Example output:

```
# ps -ef | grep sshd

root      359672      41  0 10:06 ?          00:00:00 runsv sshd
```

```

root      359673  359672  0 10:06 ?          00:00:00 /usr/sbin/sshd -D
root      362482  83084  0 10:07 pts/0    00:00:00 grep --color=auto sshd

```

20. To provide a sudo privilege for a specific active directory user, at the end of the `/etc/sudoers` file, include the following:

```
<Domain Netbios name>+<ADuser_name> ALL=(ALL) ALL
```

21. To provide a sudo privilege for all the users of an active directory group, at the end of the `/etc/sudoers` file, include the following:

```
%ActiveDirectoryUserGroup ALL=(ALL:ALL) ALL
```

Example output:

```

%Domain\ Users ALL=(ALL:ALL) ALL
%Domain\ Admins ALL=(ALL:ALL) NOPASSWD:ALL
%Linux\ Admins ALL=(ALL:ALL) NOPASSWD:ALL

```

Where, "Domain Users", "Domain Admins", and "Linux Admins" are group names in the active directory.

22. To provide `su` privileges to an active directory user, comment the following lines in the file: `/etc/pam.d/su`:

```

auth      sufficient      pam_wheel.so trust use_uid
auth      required        pam_wheel.so   use_uid

```

23. Update the password in the file: `/opt/raid/activedirectory/activedirectoryConfig.yml`:

```
Update password and domain in /opt/raid/activedirectory/activedirectoryConfig.yml
```

Example output:

```

cat /opt/raid/activedirectory/activedirectoryConfig.yml
files_to_move:
- src: activedirectory/files/smb.conf
  dest: /etc/samba/smb.conf
- src: activedirectory/files/krb5.conf
  dest: /etc/krb5.conf
- src: activedirectory/files/nsswitch.conf
  dest: /etc/authselect/user-nsswitch.conf

```

```

- src: activedirectory/files/password-auth
  dest: /etc/pam.d/password-auth
- src: activedirectory/files/sshd_config
  dest: /etc/ssh/sshd_config
- src: activedirectory/files/sudoers
  dest: /etc/sudoers
password: U29udXNAMTIz
domain: PSXAD2019.sonusqa.net

```

24. Backup the current active directory configurations to the directory `/opt/raid/`. These backed up configurations are used to retain the configurations after a RAMP upgrade:

```
/opt/raid/activedirectory/activedirectoryConfiguration.sh -a
```

Example output:

```

[2024-11-13 08:44:20 root@cmpsource: /opt/raid/activedirectory ]# /opt/raid/
activedirectory/activedirectoryConfiguration.sh -a
[2024-11-13 08:44:42 root@cmpsource: /opt/raid/activedirectory ]#
[2024-11-13 08:45:16 root@cmpsource: /opt/raid/activedirectory ]# ls -ltr files/
total 24
-rw-r-----. 1 root root  385 Nov 13 08:19 smb.conf
-rw-r-----. 1 root root 5458 Nov 13 08:20 sshd_config
-rw-r-----. 1 root root  891 Nov 13 08:21 krb5.conf
-rw-r-----. 1 root root 1845 Nov 13 08:26 password-auth
-rw-r-----. 1 root root 2976 Nov 13 08:26 nsswitch.conf
[2024-11-13 08:45:26 root@cmpsource: /opt/raid/activedirectory ]#

```

25. Enable `winbind` authentication and creation of user's home directory:

```
authselect select --force winbind with-mkhomedir
```

Example output:

```

# authselect select --force winbind with-mkhomedir
Backup stored at /var/lib/authselect/backups/2024-11-24-03-56-12.H1FwMi
Profile "winbind" was selected.
The following nsswitch maps are overwritten by the profile:
- passwd
- group

Make sure that winbind service is configured and enabled. See winbind
documentation for more information.

- with-mkhomedir is selected, make sure pam_oddjob_mkhomedir module

```

```
is present and oddjobd service is enabled and active
- systemctl enable --now oddjobd.service
```

26. To enable and start the `oddjobd` service immediately:

```
systemctl enable --now oddjobd.service
```

Example output:

```
# systemctl enable --now oddjobd.service
```

27. Apply the changes:

```
authselect apply-changes
```

Example output:

```
authselect apply-changes

Changes were successfully applied.
```

28. Verify the RAMP `ssh` login using active directory.. Refer to [Authenticating an Active Directory User](#).

Custom Host and DNS Configuration for Kubernetes Pods

Use this procedure to add the Active Directory server details to the `/etc/hosts` and `/etc/resolv.conf` files of the Ribbon Application Management Platform (RAMP) pod. To configure the `/etc/hosts` and DNS settings for a RAMP pod through the `values.yaml` file in a Helm chart, modify the RAMP Helm chart templates to inject the necessary configuration in to the pod's `/etc/hosts` and DNS settings. Once the configuration is complete, proceed with the RAMP instantiation procedure. Refer to [RAMP CNF - Standalone Deployment Using Helm Charts](#).

Start

Edit the RAMP `value.yaml` file.

Parameters with Example Values

Parameter	Example Value
Active Directory Domain name	sonusqa.net
Domain Netbios name	sonusqa
Windows Server computer name	PSXAD2019
Short Domain name	testdom
Windows Server admin user name	administrator
Linux Hostname	sanrampperf2-rampcnf-0
AD server	10.54.48.246

```
## @param activedirectory to enable activedirectory
## set enabled to true to use activedirectory
activedirectory:
  enabled: true
  hostAliases:
    - ip: "10.52.186.164"
      hostnames:
        - "sanrampperf2-rampcnf-0.sonusqa.net"
        - "sanrampperf2-rampcnf-0"
    - ip: "10.54.48.246"
      hostnames:
        - "psxad2019"
        - "psxad2019.sonusqa.net"
        - "sonusqa"
        - "sonusqa.net"
  dnsConfig:
    nameservers:
      - "10.54.48.246"
    # searches:
    # -
    # options:
    # - name: ndots
    #   value: "2"
```

Daily Maintenance Activities

This section describes activities you should perform on a daily basis on Ribbon Application Management Platform (RAMP).

Continuous Monitoring

The most important task to proactively maintain system health and performance is continuous (real-time) system-level monitoring enabled by the Ribbon Application Management Platform (RAMP) functions.

Continuous system monitoring typically includes the following activities:

- Monitor system traps and alarms using the RAMP Fault Management (FM) service. For information on isolating and troubleshooting system fault conditions, refer to [RAMP Alarms Guide](#).
- Monitor RAMP performance metrics using the RAMP Performance Management (PM) service, refer to [Performance Management](#).

Daily Maintenance Tasks

Perform the following tasks on a daily basis:

- Check uncleared RAMP alarms, and delete alarms that are not required.
- View the System Activity log by navigating to **System > Troubleshooting > System Activity** and selecting the **View Log** button.
- [Check RAMP status](#), the output should indicate that all components listed for the device are running.

Daily Database Backups

Ribbon recommends backing up the RAMP database on a daily basis. Refer to [Take a Backup of RAMP for Daily Maintenance](#).

How to Start and Stop RAMP

Start RAMP

Use this procedure to start Ribbon Application Management Platform (RAMP). If you have deployed RAMP with redundancy, perform this procedure on the active RAMP device.

1. Access RAMP as the insight user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the insight user.
2. Start RAMP:

```
/opt/sonus/ems/emsMgmt start
```

Stop RAMP

Use this procedure to stop Ribbon Application Management Platform (RAMP). If you have deployed RAMP with redundancy, perform this procedure on the active RAMP device.

1. Access RAMP as the insight user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the insight user.
2. Stop RAMP:

```
/opt/sonus/ems/emsMgmt stop
```

How to Start and Stop Sonus Agent

Use the following procedures if you are directed to stop or start the sonus agent.

To stop sonus agent:

1. Log on as the `Insight` user.
2. Issue the following command:

```
/opt/sonus/sonusComm/bin/sonusAgent stop
```

The following is a sample output:

```
-- Removing sonusAgent keep-alive cron job.  
-- Stopping sonusAgent...
```

To start sonus agent:

1. Log on as the `insight` user.
2. Change to the directory `/opt/sonus/sonusComm/bin` using the following command:

```
cd /opt/sonus/sonusComm/bin
```

3. Issue the following command:

```
./sonusAgent start
```

The following is sample output.

```
-- Starting sonusAgent ...  
-- Adding keep-alive cron job for sonusAgent.
```

How to Rediscover the localhost

Use the following procedure to rediscover the Ribbon Application Management Platform (RAMP) instance. When a RAMP instance is initially created, it automatically registers and discovers itself. However, after a configuration change, migration, backup and restore, or upgrade, it may become necessary to rediscover the localhost to ensure that the current parameters are stored. The "localhost" entry in the RAMP devices list refers to the RAMP instance itself. You can use the localhost entry to initiate a discovery of the RAMP instance if needed.

Prerequisites

- The device is up and running.
- Super User [privileges](#) for **Insight Administration** under **Core Resources**.
- **Devices** and **Resource Groups** [privileges](#) under **Device Management**.

Start

1. Log on to the RAMP GUI.
2. Navigate to **DEVICE MANAGEMENT > Devices**.
3. In the **Nodes** list row for the localhost (standalone or GR) you want to discover, click the ellipses (...) menu under **Action** and select **Discover**.
A success message displays.

Note

To edit RAMP registration parameters, refer to [Edit RAMP Device Registration](#).

How to Control the Network Range

Occasionally, the internal network assigned by the docker service is identical to the network used on your premises. This leads to a conflict in the network causing connectivity issues. In such a scenario, specify the docker service to pick the provided IP address from the pool for docker internal network.

The Ribbon Application Management Platform (RAMP) allows you to add a file `/opt/rbbn/dockerNetworksFile` through the user data if your internal network clashes with the networks created by the docker service.

This file validates and writes the data to the `/etc/docker/daemon.json` file.

Note

You must add a minimum of seven networks for the RAMP 24.03 release. You are allowed to add networks that suit you, but do not change the variable names.

IPv6 support is currently disabled.

Example code to write files

```
write_files:
  - path: /opt/rbbn/dockerNetworksFile
    permissions: '0744'
    owner: root:root
    content: |
      dockerNetwork1=172.37.0.0/16
      dockerNetwork2=172.38.0.0/16
      dockerNetwork3=172.39.0.0/16
      dockerNetwork4=172.30.0.0/16
      dockerNetwork5=172.31.0.0/16
      dockerNetwork6=172.32.0.0/16
      dockerNetwork7=172.33.0.0/16
```

Example creation of user data

```
#cloud-config
timezone: "Asia/Kolkata"
ntp:
  enabled: true
  ntp_client: chrony
  config:
```



```

confpath: /etc/chrony.conf
check_exe: chronyd
packages:
  - chrony
service_name: chronyd
template: |
  ## template:jinja
  # My NTP Client config
  {%- if servers %}# servers
  {% endif %}
  {% for server in servers -%}
  server {{server}} iburst
  {% endfor %}
servers:
  - 10.128.254.68
manage_resolv_conf: true
resolv_conf:
  nameservers: ['$dnsServer']
  searchdomains:
    - $dnsSearchPath
write_files:
  - path: /opt/rbbn/userData.json
    permissions: '0644'
    content: |
      {
        "IF1": {"GWV4": "10.11.14.1", "IPV4": "10.11.15.153/23","Port": "eth0"},
        "IF2": {"GWV4": "", "IPV4": "/", "Port": ""},
        "growpart": { "opt" : 60, "pgsql": 30, "home":10},
        "InstanceName": "VinayRamp"
      }
  owner: root:root
  - path: /opt/rbbn/dockerNetworksFile
    permissions: '0777'
    content: |
      dockerNetwork1=172.37.0.0/16
      dockerNetwork2=172.38.0.0/16
      dockerNetwork3=172.39.0.0/16
      dockerNetwork4=172.30.0.0/16
      dockerNetwork5=172.31.0.0/16
      dockerNetwork6=172.32.0.0/16
      dockerNetwork7=172.33.0.0/16
  owner: root:root
runcmd:
  - usermod -p '$1$admin$1kgWpnZpUx.vTroWPXIB0' admin
  - usermod -f -1 admin

```

How to Prepare RAMP for ROHOS Upgrade

This procedure is applicable only for KVM installed on the **Ribbon Dell servers**.
Skip this procedure if you are not using **Ribbon Dell servers**.

Use this procedure to prepare the Ribbon Application Management Platform (RAMP) for the Hypervisor upgrade:

Start

1. Back up the RAMP and copy the backup to a remote/external server. For more information, refer to [Take a Backup of RAMP for Daily Maintenance](#).
2. Shut down the RAMP. For more information, refer to [How to Start and Stop RAMP](#).
3. Ensure you note down the RAMP Virtual Machine (VM) name. If you are unaware of the VMs on your system, list the VMs on the host OS:

```
virsh list --all
```

4. Shut down the RAMP VM on the host OS:

```
virsh shutdown <VMName>
```

5. Perform the ROHOS upgrade procedure after the VM is powered off. For more information, refer to [Update Ribbon OEM Host OS Software](#).
6. Power on the VM after you complete the ROHOS upgrade.
7. Log on to the host OS.
8. Start the RAMP VM on the host OS:

```
virsh start <vm_name>
```

9. Observe that the RAMP starts automatically after the VM booted successfully.
10. Check the RAMP running status. For more information, refer to [Check RAMP Status](#).
11. If the RAMP fails to start, perform the [How to Start and Stop RAMP](#) procedure, to start it manually.
12. Ensure you can log in to the RAMP GUI through <https://<RAMP_IP>.

Access RAMP Database

Use this procedure to access the Ribbon Application Management Platform (RAMP) database.

Start

1. SSH to the RAMP device as the `admin` user.
2. Change to the `postgres` user:

```
sudo su - postgres
```

3. Enter the following command:

```
psql -U dbimpl -d dbimpl -h <The IP address of the RAMP host>
```

The following is an example:

```
psql -U dbimpl -d dbimpl -h 127.0.0.1
```

The following prompt displays:

```
Password for user dbimpl:
```

For the default `dbimpl` password, refer to [Manage RAMP Account Names and Passwords](#).

4. Enter the `dbimpl` password. Now you can enter postgres (RAMP database) commands.

Attach RAMP to Multiple Disjointed IP Networks

Related articles:

- [Using RAMP as a PSX Proxy](#)
- [Separation of OAM and Signaling Networks on Call Trace in RAMP](#)

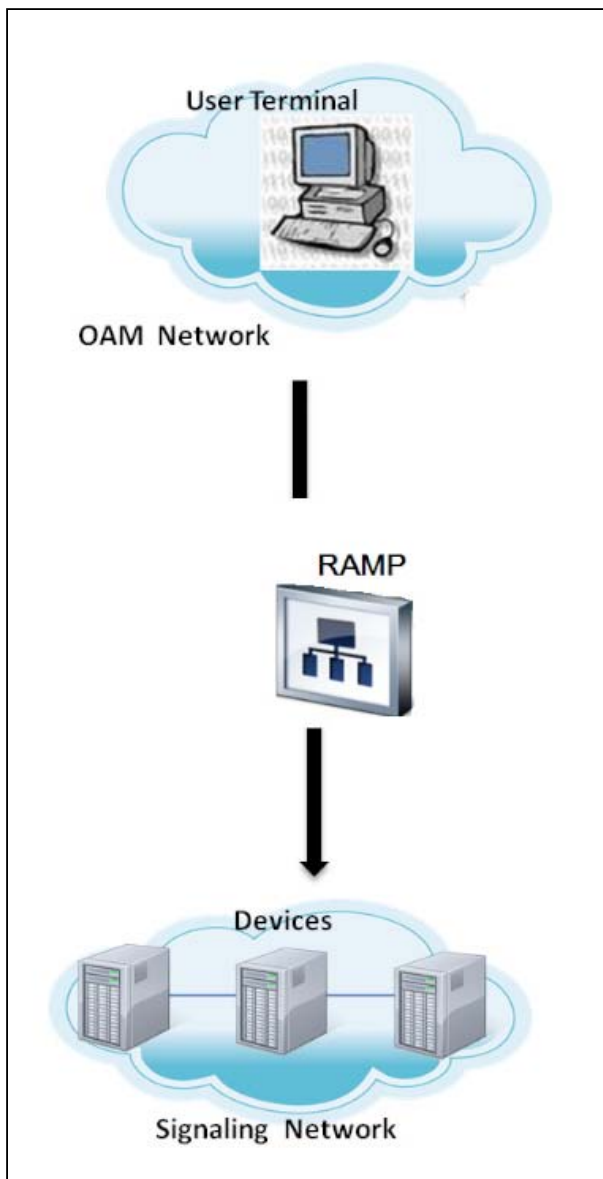
Many Internet Protocol (IP) networks provide any-to-any connectivity between any two endpoints. In such an environment, a single point of attachment (Ethernet port) is required for all IP connectivity. Some IP networks, however, are configured to be segmented and disjointed from other networks for security or performance reasons. In such an environment, some nodes may need to be attached to more than one of the disjointed networks. Examples of such dedicated networks include:

- **Operations, Administration, and Management (OAM) Network** — where NOC personnel or other users may reside and access Ribbon Application Management Platform (RAMP) GUI/API/CLI services.
- **Service/Signaling Network** — where core network equipment (PSX, SBC, DSI, and so on) provide services.
- **Backup/Restoration or VM Network** — where large periodic traffic flows are isolated from other networks. The interface on this subnet is also used to backup data from the RAMP.

RAMP on OpenStack supports multiple interfaces. This handles the Lawful Interface (LI) communication on the eth1 interface. The following diagram uses a single interface to manage the devices.

IP Multimedia Subsystem (IMS) LI is not supported on the eth1 interface.

RAMP in customer network



Using RAMP as a PSX Proxy

If separate networks are configured for OAM and service equipment, then Ribbon Application Management Platform (RAMP) may need to be configured as a proxy server, so that the PSX Manager can connect to PSX through the RAMP host acting as a proxy.

In a standalone RAMP deployment with two different networks for OAM and service/signaling, PSX Manager connects to RAMP through the RAMP OAM IP address, if PSX proxy mode is enabled..

Ribbon Application Management Platform (RAMP) acts as a proxy server for both the PSX Manager and the PSX server to maintain a secured communication. If a direct/unsecured connection to PSX connection is preferred, then change the following settings as per the following table.

The proxy from RAMP is only supported for PSX Manager. The proxy is not supported for 4331 (PSX manager test db), 5330 (PSX manager shadow mode), and 3091 (ssreq).

For RAMP GR, configure active and standby nodes to act as proxy servers.

PSX Proxy parameters

Parameter	Description	Values
psxProxyEnabled	Set RAMP to act as a proxy server for PSX Manager and the PSX server. Note The parameter <code>sslProxyEnabled</code> takes precedence over <code>psxProxyEnabled</code>. If <code>psxProxyEnabled</code> is set to false and <code>sslProxyEnabled</code> is set to true RAMP uses TLS. Set the flag to false if you need a direct connection from PSX Manager to the PSX server. If you disable the <code>psxProxyEnabled</code> flag, the network traffic is not secure.	• true • false
sslProxyEnabled	Use the cryptographic protocol to secure traffic from PSX Manager to RAMP. If you set this flag to false, the traffic from PSX manager to RAMP is not secure. Note The connection uses TLS not SSL. RAMP uses the <code>sslProxyEnabled</code> variable to determine whether to establish a TLS connection. Note If <code>sslProxyEnabled</code> is set to true, for non-cloud nodes provide direct SSH login credentials in the PSX node registration page to secure the communication between RAMP and PSX.	• true • false

To configure **RAMP** to act as a proxy server, install SSH on both systems and edit the file `/opt/sonus/ems/weblogic/sonusEms/data/sys/SystemConfig.txt`. Set the following parameters in the `SystemConfig.txt`.

RAMP can act as a proxy server for both the PSX Manager and the PSX server. In such a configuration, the traffic diagram involves PSX Manager <> Insight <> PSX.

The protocol used is Ribbonproprietary PIPE messaging. You can secure the traffic from the PSX Manager to RAMP using TLS and the traffic from RAMP to the PSX using SSH.

Parameters in SystemConfig.txt

Parameter	Default Setting	Change to	
psxPorts	4330 (PSX manager PIPE server) 4331 (PSXmanagertestdb) 5330 (PSX manager shadow mode) 3091 (ssreq)	Add or change the PSX ports that the proxy is allowed to connect based on your system-wide policy server configuration.	
tcpListenPort	9000	Change only if using a different port.	—
sslListenPort	9001	Change only if using a different port.	—
proxyPreferredIp	none	This parameter allows you to set the IP address that RAMP uses when launching the PSX Mgr. Add this parameter only if RAMP has multiple IP addresses and the client workstations cannot reach the default IP address. If all PSX Mgr launch traffic is to be sent to RAMP on only an IP address then set this proxyPreferredIp in SystemConfig.txt to this IP address. Set this parameter to the well-known IP address or to the fully qualified domain name. Also, verify that all RAMP client workstations are reachable at this IP address or domain name.	
	Standalone Mode	Single Public IP	M u l t i p l e P u b l i c I P

Parameter	Default Setting	Change to	
		none	Manually configure the IP that is used by the GUI clients.

Parameter	Default Setting	Change to	
proxyPreferredIp2	none	It is potentially a second IP address used to launch the PSX Mgr depending on the IP configuration of the launching PC and RAMP. These two settings can contain an IP address (or name such as "localhost") and an optional port. If the PSX Mgr traffic is sent to RAMP on an IP address and port, defining proxyPreferredIp and proxyPreferredIp2 depends on the RAMP destination port. If the destination port is 443, which is https traffic, then define proxyPreferredIp to route to this port on RAMP. All subsequent traffic between the PSX Mgr and RAMP will be non-https traffic. proxyPreferredIp2 will need to be set to the same IP address or name but with a different port. This port may be 9001 which is for the RAMP SSH tunnel between the PSX Mgr and PSX. proxyPreferredIp and proxyPreferredIp2 can specify ports to enable communication with a tunnel configuration on the PC. For example, if the PC is on an IPv4 network and uses a jump-station to connect to RAMP IPv6 network: • local port 9990 is used to connect to the RAMP port 443 • local port 9991 is used to connect to the RAMP port 9001 proxyPreferredIp=localhost:9990 It will be matched with this Putty SSH tunnel on the PC (if the IPv6 RAMP address is 2000:184::10:158:184:30): L9990 [2000:184::10:158:184:30]:443 proxyPreferredIp2=localhost:9991 It will be matched with this Putty SSH tunnel on the PC (if the IPv6 RAMP address is 2000:184::10:158:184:30): L9991 [2000:184::10:158:184:30]:9001 The login to RAMP is initiated through https://localhost:9990/ and the PSX Mgr java application uses port 9001 between the jumpstation and RAMP.	

Parameter	Default Setting	Change to	
	Standalone Mode	Single Public IP	M u l t i p l e P u b l i c I P
		none	M a n u a l l y c o n f i g u r e t h e I P t h a t i s u s e d b y t h e G U I c l i e n t s.

After making the changes, you must stop and restart RAMP.

You also need to properly configure the Node Registration information for RAMP and the PSX on the Node Registration pages.

Refer to [Register a PSX Device](#) and [Edit RAMP Device Registration](#).

Separation of OAM and Signaling Networks on Call Trace in RAMP

The section describes a scenario where the signaling and OAM networks are separated out, and necessary updates in Ribbon Application Management Platform (RAMP) is performed to support this network.

RAMP communicates with DSI/GSX using OAM network interface. However, GSX can communicate with DSI/NFS using Signaling network.

The IP Address from the Signaling network interface are configured as primary and secondary NFS address on the RAMP node registration of the GSX.

DSI has two interfaces. One interface on OAM network for communicating with **RAMP** and other interface on Signaling network for communicating with **GSX**.

For any **GSX** CDRs, CTRs, and PIF operations, **RAMP** fetches the IP address of the configured DSI/NFS from the **GSX**.

Since **GSX** is connected to DSI using a signaling network, **GSX** responds to **RAMP** with the signaling IP of DSI when the query for DSI is configured.

Note

Call Trace Reports and Call Data Reports work in both DSI-NFS and DSI - Streaming Mode. However, PIF works only with the DSI-NFS Mode.

By default, Node registry searches only the default and secondary IPs provided during registration to search a node.

By enabling the Alternate IP Address field, you can retrieve all IPs configured for that node.

RAMP has complete list of reachable and non-reachable IPs of a node.

This enables **RAMP** to use reachable IPs of DSI even when **GSX** provides us with non-reachable IPs of DSI by comparing with the available IP list for the respective DSI.

Backup and Restore

This section includes the following Ribbon Application Management Platform (**RAMP**) backup and restore operations. These procedures also apply to the **RAMP** Cloud Native Functionality (CNF).

- [Take a Backup of RAMP for Daily Maintenance](#)
- [Take a Backup of RAMP for Upgrade](#)
- [Restore from Backup on RAMP Standalone](#)
- [Restore from Backup on RAMP GR](#)
- [Restore a Master Key File](#)
- [Restore a Master Key File \(.KF\) Manually](#)

Take a Backup of RAMP for Daily Maintenance

Use this procedure to backup the Ribbon Application Management Platform (**RAMP**) database. For **RAMP** Geographically Redundant (GR) deployments, perform this procedure on the active (source) device.

As a security measure, when backing up the database, you have the option to store the master key encryption file in a remote location separate from other backup files. To enable this option, you must generate a template file that identifies the remote location for the master key file and provide the password to access the location.

Taking a backup of the **RAMP** database does not affect other services on **RAMP**.

- The insight password is retained after restoring the backup.
- The admin password is not retained after restoring the backup; use the default password "admin" after restoring a backup and refer to [Managing RAMP Users and Accounts](#) for information on changing the password.

Prerequisites

- A host is available to store the backup files.

Note

Ensure the following folders are empty:

`/opt/raid/devmgmtbkp`

`/var/lib/pgsql/13/backups`

`/var/lib/pgsql/12/backups`

Start

1. Access RAMP as the `root` user. Refer to [Log onto the RAMP CLI](#) to access the RAMP as the `root` user.
2. Create a directory for storing backup files on the RAMP. Ensure that this directory has sufficient space for the backup files.
 - a. For cloud-based RAMP devices, use a directory under `/opt/raid`.
 - b. For non-cloud RAMP devices, use a directory under `/opt`. The following is an example:

```
mkdir -p /opt/raid/backup
```

3. (Optional) If you want to back up the master key file in a remote location, complete the following:
 - a. Navigate to the following directory:

```
cd /opt/rbbn/ems/conf/
```

- b. Generate a template file that contains backup configuration options for the key file:

```
./manualBackup.sh -g
```

Sample output

```
Generating template /opt/sonus/ems/./secureKFBackup.conf
Template Generation complete /opt/sonus/ems/./secureKFBackup.conf
```

- c. Establish a `passwordless` connection between RAMP and the remote location to which you are backing up the key file. Refer to [Establish Passwordless Connection from an External Server to RAMP](#).
- d. Edit the `/opt/sonus/ems/./secureKFBackup.conf` template file for your backup parameters:

Template file secureKFBBackup.conf

```
IP=<The IP address of the remote server.>
User=root
remote_master_key_location=<The location of the remote_master_key.>
Secure_Master_Key=true
Secure_Option=AUTOMATIC
master_key_filename=
```

Refer to the following descriptions to set the file parameters:

- `IP` - The IP address of the remote location.
- `user` - The user name to use to access the remote location to store the backup.
- `master_key_filename` - Name of the master key file to store in the secure location.

Note

The master key file name is generated automatically by the manualBackup.sh script.

- `remote_master_key_location` - The path to the remote storage location.

Note

Ensure that the path to the remote location is accessible.

- `Secure_Master_Key` - Use `true` to specify to secure the master key file separately. The available options are, "true" and "false".
- `Secure_Option` - Use AUTOMATIC to specify to store the file automatically. The available options are, "AUTOMATIC" and "MANUAL."

Example of an edited file:

```
IP=10.54.28.89
user=root
remote_master_key_location=/opt/backup
Secure_Master_Key=true
Secure_Option=AUTOMATIC
master_key_filename=
```

Note

You must provide valid data in the configuration file. Otherwise, a secure backup of the master key file will fail.

- e. Save and exit the template file.

- f. Initiate a backup with a separate master key file:

```
/etc/sonus/manualBackup.sh -b -s -d <path to backup directory>
```

Example:

```
/etc/sonus/manualBackup.sh -b -s -d /opt/raid/backup
```

When prompted, confirm that you want to take a backup of the `pm_archive` file.

When prompted, provide the password to the remote location for the master key file.

When prompted, confirm if you want to take a backup of inventory reports.

4. To initiate a backup:

- Initiate a backup without a separate master key file:

```
/etc/sonus/manualBackup.sh -b -d <path to backup directory>
```

Example output:

```
# /etc/sonus/manualBackup.sh -b -d /opt/raid/
All backup will be taken.
Taking FM backup
Taking backup of fmdb
-----

1. Taking FM Backup
-----

FM Backup /opt/raid//FMDBBackup.tar created successfully
Removing FMDB backup
FMDB backup is successful. 'FMDBBackup.tar' is created under /opt/raid/
Taking PM backup
Taking backup of pmdb
PMDB backup is successful. 'PMDBBackup.tar' is created under /opt/raid/
Taking LM backup
Taking backup of LM
Starting LM Database backup
dbaas_post_install licmdb successful
Taking backup of licmdb
licmdb backup successful
Backup Completed, File present at /opt/raid//LMBackup.tar
LM backup is successful. 'LMBackup.tar' is created under /opt/raid/
Taking DEVMGMT backup
Taking backup of devmgmtdb
DMDB backup is successful. 'DEVMEGMDDBBackup.tar' is created under /opt/raid/
Taking ACS backup
Taking backup of ACS
```

```

Action Service Marker does not exist. Skipping action service backup.
Taking Object Store Service backup
Taking backup of Object Store Service
Object Store Service Marker does not exist. Skipping object store service
backup.
Taking Notification Service Backup
Taking backup of Notification Service
Notification Service Marker does not exist. Skipping notification service
backup.
Taking Global Search Service Backup
Taking backup of Global Search Service
Global Search Service Marker does not exist. Skipping Global Search Service
backup.
Taking AA backup
Taking backup of AA
AA backup is successful. 'AABackup.tar' is created under /opt/raid/
Taking Insight backup
Generating deployed service list
Taking backup of insight from Postgres database
Insight backup is successful. 'backupFiles.tar' is created under /opt/raid/
Updating Backup with FM backup
Updating Backup with PM backup
Updating Backup with LM backup
Updating Backup with DM backup
Updating Backup with AA backup

Backup procedure completed successfully.Check /opt/sonus/ems/logs/
manualBackup.log for more details.

[2024-12-09 08:42:55 root@sanramp04: /home/admin ]#

```

5. Copy the backup files to a remote server.

Note

Do not change any configuration on RAMP until the backup operation is complete.

The following table summarizes the parameters available with the script `manualBackup.sh` :

Options for manualBackup.sh

Parameter	Optional (O) / Mandatory (M)?	Description
-b	M	Generate the backup file.
-d	M	Directory to copy the configuration files.
-e	O	Take a backup of EdgeView.
-f	O	Take a backup of Fault Management.

Parameter	Optional (O) / Mandatory (M)?	Description
-i	O	To take a backup of the insight.
-g	O	Specify to generate a configuration template for securely backing up the master Key file. Use this separately from other options.
-l	O	Take a backup of License Management.
-n	O	Take a backup of the Device Manager.
-m	O	For migration.
-o	O	Object Store Service backup.
-j	O	Notification Service backup.
-p	O	Take a backup of Performance Management.
-q	O	Exclude the pm-archive folder in the backup tar without manually answering.
-Q	O	Exclude the pm-parquet folder in the backup tar without manually answering, without -Q, the pm-parquet will be backedup
-r	O	Include the dm inventory reports folder in the backup tar without manually answering.
-s	O	Secure a backup of the master key.
-t	O	Exclude the dm inventory reports folder in backup tar without manually answering.
-u	O	ACS backup.
-x	O	Include the pm-archive folder in backup tar without manually answering.

To restore the backup, perform one of the following:

- For RAMP standalone, refer to [Restore from Backup on RAMP Standalone](#).
- For RAMP GR, refer to [Restore from Backup on RAMP GR](#).

Take a Backup of RAMP for Upgrade

Use the following procedure to take a backup of the Ribbon Application Management Platform (RAMP) database. For RAMP Geographically Redundant (GR) deployments, perform this procedure on the active (source) device.

As a security measure when backing up the database, you can store the master key encryption file in a remote location separate from other backup files. To enable this option, generate a template file that identifies the remote location for the master key file and provide the password to access the location.

Taking a backup of the RAMP database does not affect other services on RAMP.

- The insight password is retained after restoring the backup.
- The admin password is not retained after restoring the backup. Use the default password "admin" after restoring the backup. For more information on password changes, refer to [Managing RAMP Users and Accounts](#).

Prerequisites

- A host is available to store the backup files.

Start

1. Access RAMP as the "root" user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the "root" user.
2. Upgrading from 21.11 and 22.02 to 23.0x:
 - a. Perform the pre-upgrade/pre-backup steps on the current RAMP 21.11/22.02 node.
 - i. Download the latest RAMP `rampBootstrap.tar` to RAMP 21.11/22.02.
 - ii. `tar xvf <rampBootstrap.tar> correctLmCsd.sh`
 - iii. `./correctLmCsd.sh`
 - b. Take a backup. For more information, refer to [Take a Backup of RAMP for Daily Maintenance](#).
3. To upgrade from release 22.12 and onwards, continue to the next step.
4. Create two directories.
 - a. Create a directory for storing backup files in RAMP. Ensure that this directory has sufficient space for the backup files. For non-cloud RAMP devices, use a directory under `/opt/sonus`.
 - b. Create a directory for copying bootstrap files.

Example

```
mkdir -p /opt/sonus/backup
mkdir -p /opt/sonus/BootStrap
```

5. Navigate to the BootStrap directory:

```
cd /opt/sonus/BootStrap
```

6. Download the `rampBootstrap-V<version>.tar` file for the target RAMP version.
7. Extract the `rampBootstrap-V<version>.tar` file: where <version> is the RAMP version to which you are upgrading.


```
tar -xvf rampBootstrap-V<version>.tar
```

8. Initiate a backup without a separate master key file: `/opt/sonus/BootStrap/manualBackup.sh -b -d <path to backup directory>`.

```
/opt/sonus/BootStrap/manualBackup.sh -b -d /opt/sonus/backup
```

9. Back up the master key in a remote location:

Note

This step is not needed if you perform step 8.

- a. Generate a template file that contains backup configuration options for the key file:

```
./manualBackup.sh -g
```

Sample output

```
Generating template /opt/sonus/ems/./secureKFBackup.conf
Template Generation complete /opt/sonus/ems/./secureKFBackup.conf
```

- b. Establish passwordless connection between RAMP and the remote location to which you are backing up the key file. Refer to [Establish Passwordless Connection from an External Server to RAMP](#).
- c. Edit the `/opt/sonus/ems/./secureKFBackup.conf` template file for your backup parameters:

Template file secureKFBackup.conf

```
IP=<The IP address of the remote server.>
User=root
remote_master_key_location=<The location of the remote_master_key.>
Secure_Master_Key=true
Secure_Option=AUTOMATIC
master_key_filename=
```

Refer to the following descriptions to set the file parameters:

- `IP` - The IP address of the remote location.
- `user` - The user name to use to access the remote location to store the backup.
- `master_key_filename` - Name of the master key file to store in the secure location.

Note

The master key file name is generated automatically by the manualBackup.sh script.

- `remote_master_key_location` - The path to the remote storage location.

Note

Ensure that the path to remote location is accessible.

- `Secure_Master_Key` - Use true to specify to secure the master key file separately. Options available are "true" and "false".
- `Secure_Option` - Use AUTOMATIC to specify to store the file automatically. Options are "AUTOMATIC" and "MANUAL."

The following is an example of an edited file:

```
IP=10.54.28.89
user=root
remote_master_key_location=/opt/backup
Secure_Master_Key=true
Secure_Option=AUTOMATIC
master_key_filename=
```

You must provide valid data in the configuration file. Otherwise, secure back up of the master key file will fail.

- d. Save and exit the template file.
- e. Initiate a backup with a separate master key file:

```
/opt/sonus/BootStrap/manualBackup.sh -b -s -d <path to backup directory>
```

Example

```
/opt/sonus/BootStrap/manualBackup.sh -b -s -d /opt/sonus/backup
```

When prompted, provide the password to the remote location for the master key file.

10. When prompted, confirm that you want to take a backup of the pm_archive file.
11. When prompted, confirm that if you want to take a backup of inventory reports.

The following is sample output from a backup where the master key file is stored separately:

All backup will be taken.

Taking FM backup

Taking backup of fmdb

1. Taking FM Backup

FM Backup /opt/sonus/backup//FMDBBackup.tar created successfully

Removing FMDB backup

FMDB backup is successful. 'FMDBBackup.tar' is created under /opt/sonus/backup/

Taking PM backup

Taking backup of pmdb

Do you wish to take backup of pm_archive, Confirm [Y|y, N|n] ?

n

PMDB backup is successful. 'PMDBBackup.tar' is created under /opt/sonus/backup/

Taking LM backup

Taking backup of LM

Starting LM Database backup

dbaas_post_install licmdb successful

Taking backup of licmdb

licmdb backup successful

Backup Completed, File present at /opt/sonus/backup//LMBBackup.tar

LM backup is successful. 'LMBBackup.tar' is created under /opt/sonus/backup/

Taking DEVMGMT backup

Taking backup of devmgmtdb

Do you wish to take backup of inventory reports, Confirm [Y|y, N|n] ?

y

DMDB backup is successful. 'DEVMEGMDTDBBackup.tar' is created under /opt/sonus/backup/

Taking backup of EV

evDBBackup

EV backup is successful. 'evDBBackup.tar' is created under /opt/sonus/backup/

Taking AA backup

Taking backup of AA

AA backup is successful. 'AABBackup.tar' is created under /opt/sonus/backup/

Taking Insight backup

Generating deployed service list

/bin/tar: Removing leading '/' from member names

/bin/tar: Removing leading '/opt/sonus/../../' from member names

deployed_list.txt

Taking backup of insight from Postgres database

Insight backup is successful. 'backupFiles.tar' is created under /opt/sonus/backup/

Updating Backup with FM backup

Updating Backup with PM backup

Updating Backup with LM backup

Updating Backup with DM backup

Updating Backup with EV backup

Updating Backup with AA backup

Backup procedure completed successfully. Check `/opt/sonus/ems/logs/manualBackup.log` for more details.

12. Copy the backup files to a remote server.

Do not change any configuration on **RAMP** until the backup operation is complete.

The following table summarizes the parameters available with the script `manualBackup.sh`.

manualBackup.sh Options

Parameter	Optional (O) / Mandatory (M)?	Description
-b	M	Generate the backup file.
-d	M	Directory to copy the configuration files.
-e	O	Take a backup of EdgeView.
-f	O	Take a backup of Fault Management.
-i	O	To take a backup of the insight.
-g	O	Specify to generate a configuration template for securely backing up the master Key file. Use this separately from other options.
-l	O	Take a backup of License Management.
-n	O	Take a backup of the Device Manager.
-m	O	For migration.
-o	O	Object Store Service backup.
-p	O	Take a backup of Performance Management.
-q	O	Exclude the pm-archive folder in backup tar without manually answering.
-r	O	Include the dm inventory reports folder in the backup tar without manually answering.
-s	O	Secure a backup of the master key.

Parameter	Optional (O) / Mandatory (M)?	Description
-t	O	Exclude the dm inventory reports folder in backup tar without manually answering.
-u	O	ACS backup.
-x	O	Include the pm-archive folder in backup tar without manually answering.

To restore the backup, perform one of the following:

- For RAMP standalone, refer to [Restore from Backup on RAMP Standalone](#).
- For RAMP GR, refer to [Restore from Backup on RAMP GR](#).

Restore from Backup on RAMP Standalone

Use this procedure to restore a Ribbon Application Management Platform (RAMP) instance from a backup.

If you are restoring the backup to a new RAMP instance, the instance must include the same IP address. If the RAMP hostname is changed, manually add the insight ssh key for RAMP on every PSX at `/export/home/ssuser/.ssh/authorized_keys`.

When you restore from a backup, RAMP does not restore the following:

- Configurations associated the RHEL operating system.
- Custom Cron jobs created by RAMP users.
- Custom scripts or jobs deployed at the Linux level.

Prerequisites

- [Backup](#) files are available.
- If you have stored the master key file (.KF) separately from RAMP backup data, refer to [Restore a Master Key File](#) to collect the configuration file details that identify where to retrieve the .KF file from a remote location where it is backed up.

The Action service is enabled by default only if the backup file contains both the Action and EdgeView (EV) service tar files in the RAMP backup. If the backup file contains only the Action service tar file, then Action will not be available after the 24.03R1 upgrade.

Note

Ensure the following folders are empty:

```
/opt/raid/devmgmtbkp
```

```
/var/lib/pgsql/13/backups
```

```
/var/lib/pgsql/12/backups
```

Start

1. Access **RAMP** as the root user. Refer to [Log onto the RAMP CLI](#) for accessing **RAMP** as the root user.
2. Restore from a backup:

```
/etc/sonus/emsRestore.sh -b <Location of the directory that contains the backup.>
```

Example:

```
/etc/sonus/emsRestore.sh -b /opt/sonus/backup/
```

The following output displays:

```
....
```

```
Do you wish to continue [y|Y,n|N] ?
```

3. Enter "Y".

```
Checking if backupFiles.tar is present under "/opt/sonus/backup/"
```

```
.....
```

```
.....
```

```
Insight has been started
```

```
The Sonus Insight migration is complete. Check /opt/sonus/ems/logs/emsRestore.log  
for more details.
```

4. Rediscover the localhost, refer to [How to Rediscover the localhost](#).

You can use the command `emsRestore.sh` with the following options.

usage: `emsRestore.sh [-s] [-b backupDir] [-p proxyPreferredIp] [-h]`

Parameter	Optional (O) / Mandatory (M)?	Description
-b	M	Usage: -b <backup the directory of backupFiles.tar>
-p	O	Usage: -p <the proxy preferred IP address> Format to use: ./emsRestore.sh -b <backup dir location> -p <proxy preferred IP> Example: ./emsRestore.sh -b <backup dir location> -p <proxy preferred IP>
-s	O	Silent mode execution if used with b option. Format to use: ./emsRestore.sh -s -b <path for the backup files>
yes	O	Run restore operation in the background. Command: yes ./emsRestore.sh -b <path for the backup files> & Example: yes ./emsRestore.sh -b </opt/sonus/backup> & NOTE: This option is recommended only if you encounter a connection timeout error. The restore operation continues in the background even if a session timeout occurs.
-h	O	usage: emsRestore.sh -h

Restore from Backup on RAMP GR

Use this procedure to restore a Ribbon Application Management Platform (RAMP) geographically redundant (GR) deployment from backup files..

If you are restoring from backup to a new RAMP instance, the instance must include the same IP address. If the RAMP hostname is changed, manually add the `insight` ssh key for RAMP on every PSX at `/export/home/ssuser/.ssh/authorized_keys`.

When you restore from backup, RAMP does not restore the following:

- Configurations associated with the RHEL operating system.
- Custom Cron jobs created by RAMP users.
- Custom scripts or jobs deployed at the Linux level.

Prerequisites

- Backup files are available.

Note

Ensure the following folders are empty:

```
/opt/raid/devmgmtbkp
```

```
/var/lib/pgsql/13/backups
```

```
/var/lib/pgsql/12/backups
```

Start

1. On the active (source) instance, access RAMP as the `root` user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the `root` user.
2. Restore from backup:

```
/etc/sonus/emsRestore.sh -b <Location of the directory that contains the backup.>
```

The following is an example:

```
/etc/sonus/emsRestore.sh -b /opt/raid/backup/
```

The following output displays:

```
.....
```

```
All existing Insight-controlled passwords on this box will be wiped out and
replaced with the passwords from the restored data.
```

```
#####
#####
```

```
Do you wish to continue [y|Y,n|N] ?
```

3. Enter "Y".

```
Checking if backupFiles.tar is present under "/opt/raid/backup/"
```

```
Redundancy Setup Detected; Will have to Tear-Down the setup. Do you want to
continue [y|Y,n|N]? (Default:N)
```

4. Enter "Y". The following is sample output:

```
Tearing down the setup...
```

```
.....
.....
```



```
Do you want to switch back to Redundancy Setup [y|Y,n|N]? (Default:Y)
```

5. Enter "y" and press **ENTER**. The following is sample output:

```
....
Please enter Password of admin user for all nodes (press ENTER if SSH Passwordless
login has been setup) ->
```

6. Enter the `admin` password, or press ENTER if SSH password-less login has been setup. The following is sample output:

```
[21:40:23] Building RD configuration locally .....
```

```
.....
Do you want to proceed with this setup (yes|no)? ->
```

7. Enter "yes" and press **ENTER**. The following is sample output:

```
[21:40:25] Proceed setting up the cluster with accepted configuration .....
```

```
.....
Restoring the passwords on peer nodes...
```

```
The Sonus Insight migration is complete. Check /opt/sonus/ems/logs/emsRestore.log
for more details.
```

8. Rediscover the localhost, refer to [How to Rediscover the localhost](#).

The following table summarizes the options you can use with the command `emsRestore.sh`.

emsRestore.sh Options

Parameter	Optional (O) / Mandatory (M)?	Description
-b	M	The directory for backupFiles.tar.
-p	O	Update proxy preferred IP address.
-s	O	Silent mode if used with the b option
-h	O	Lists the help topics.

Restore a Master Key File

While performing a Ribbon Application Management Platform (RAMP) backup, you can back up and store the master key file (.KF) separately from other files on a remote machine. Refer to [Take a Backup of RAMP for Daily Maintenance](#).

If you have stored the master key file (.KF) separately from RAMP backup data, follow this procedure to collect the configuration file details and the .KF file from the remote machine.

To find the remote location details, copy the `backupFiles.tar` file to the `/tmp` directory and perform the following steps:

1. Issue the following command:

```
/bin/tar -xvf /tmp/backupFiles.tar /opt/rbbn/secureKFBackup.conf
```

- If the following error message is displayed, then the backup was taken with the master key file in it. Follow [Restore a Master Key File \(.KF\) Manually](#).

Error

```
/bin/tar: opt/rbbn/secureKFBackup.conf: Not found in archive  
/bin/tar: Exiting with failure status due to previous errors
```

- If the following message is displayed, then the configuration file was extracted. Go to **Step 2**.

Error

```
/bin/tar: Removing leading `/' from member names  
/opt/rbbn/secureKFBackup.conf
```

2. Execute the following command to view the configuration properties:

```
/bin/cat /tmp/opt/rbbn/secureKFBackup.conf
```

Review the parameter settings and perform one of the following:

- If the parameters are set as "`Secure_Master_Key=true`" and "`Secure_Option=AUTOMATIC`"
 - i. Perform [Establish Passwordless Connection from an External Server to RAMP](#) with the specified IP address.
- If the parameters are set as "`Secure_Master_Key=true`" and "`Secure_Option=MANUAL`" :
 - i. Refer to [Restore a Master Key File \(.KF\) Manually](#) to restore.

Note

The system prompts to restore the master key file manually from the remote machine to the location `/opt/rbbn/ems/weblogic/sonusEms/data/sys` as the .KF file during the restoration process.

Restore a Master Key File (.KF) Manually

To restore a master key file (.KF) manually from Ribbon Application Management Platform (RAMP) backup files:

1. If you are using an SSH session to RAMP, disable the SSH client session timeout:

- a. As the root user, navigate to the directory `/etc/ssh`
- b. Modify the file `sshd_config` to set the value of `ClientAliveInterval` to 0.

Note down the original value of `ClientAliveInterval` to reset the original value later.

- c. Restart the `sshd` service by issuing the following:

```
systemctl restart sshd
```

2. Create a directory under `/opt/rbbn/<directory name>`.
3. Copy the `backupFiles.tar` file to the directory `/opt/rbbn/<directory name>`.
4. Issue the following commands:

```
cd /opt/rbbn/ems/conf/jumpstart
```

```
./emsRestore.sh -b /opt/rbbn/<directory name>
```

The following message displays:

```
#####
#####
You are going to migrate a previous RAMP onto this system. Please make sure you
understand what you are
doing. Before you proceed, you should also have already run manualBackup.sh on the
system you want to
migrate from, which generated backupFiles.tar

All existing Insight-controlled passwords on this box will be wiped out and
replaced with the passwords from the restored data.
#####
#####

Do you wish to continue [y|Y,n|N] ?
```

5. Enter "y."
- The following message displays:

```
Stopping running Insight...
Restore the securely backed up Master Key and the process will resume
automatically.
```

The RAMP restoration process resumes once the master key file is restored.

The following message displays:

Restoring data from Migrated backup. This will take a **while**

Database has been successfully restored

6. If you are using an SSH session to RAMP, reset the SSH client session timeout:
 - a. As the root user, navigate to the directory `/etc/ssh`
 - b. In the file `sshd_config`, reset `ClientAliveInterval` to its original value.
 - c. Restart the service by issuing the following:

```
systemctl restart sshd
```

Check Software Versions

In this section:

- [Check RAMP Version](#)
- [Check LINTEL Platform Version in RAMP](#)
- [Check Red Hat Enterprise Linux Server Version in RAMP](#)
- [Check PostgreSQL Version in RAMP](#)
- [Check Java Version in RAMP](#)
- [Check DBaaS Version in RAMP](#)
- [Check Platform Kernel Version in RAMP](#)

Check RAMP Version

Use this procedure to check the Ribbon Application Management Platform (RAMP) release version.

Start

1. SSH to RAMP. To access RAMP through SSH, refer to [Log onto the RAMP CLI](#).
2. Enter the following command as the root, admin, or insight user:

```
rpm -qa SONSems
```

Check LINTEL Platform Version in RAMP

Use this procedure to check the Linux platform version in Ribbon Application Management Platform (RAMP).

Start

1. SSH to the RAMP device as the admin user.

You can enter the command in step 2 as the root, admin, or insight user.

2. Enter the following command:

```
cat /etc/os_version
```

Check Red Hat Enterprise Linux Server Version in RAMP

Use this procedure to check the Red Hat Enterprise Linux Server version on Ribbon Application Management Platform (RAMP).

Start

1. SSH to the RAMP device as the admin user.

You can enter the command in step 2 as the root, admin, or insight user.

2. Enter the following command:

```
cat /etc/redhat-release
```

Check PostgreSQL Version in RAMP

Use this procedure to check the PostgreSQL database version on Ribbon Application Management Platform (RAMP).

Start

1. SSH to the RAMP device as the admin user.
2. Change to the postgres user.

```
sudo su - postgres
```

3. Enter the following command:

```
postgres -V
```

Check Java Version in RAMP

Use this procedure to check the Java Virtual Machine (JVM)/RPM Package Manager (RPM) version on Ribbon Application Management Platform (RAMP).

Start

1. SSH to the RAMP device as the admin user.

Note

You can enter the command in step 2 and step 3 as the root, admin, or insight user.

2. To check the Java Server version:

```
java -version
```

3. To check the Java RPM Package Manager (RPM) version:

```
rpm -qa | grep -i jdk
```

Check DBaaS Version in RAMP

Use this procedure to check the Database-as-a-Service (DBaaS) version on Ribbon Application Management Platform (RAMP).

Start

1. SSH to the RAMP device as the admin user.

You can enter the command in step 2 as the root, admin, or insight user.

2. Enter the following command:

```
rpm -qa | grep dbaas
```

Check Platform Kernel Version in RAMP

Use this procedure to check the platform kernel version on Ribbon Application Management Platform (RAMP).

Start

1. SSH to the RAMP device as the admin user.

You can enter the command in step 2 as the root, admin, or insight user.

2. Enter the following command:

```
uname -r
```

Check Status

In this section:

- [Check RAMP Status](#)
- [Check Deployment Status of Services in RAMP](#)

Check RAMP Status

Use this procedure to check the status of Ribbon Application Management Platform (RAMP). If you have deployed RAMP with redundancy, perform this procedure on the active RAMP device.

All processes/services on the RAMP device automatically start after installation is complete.

1. Access RAMP as the insight user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the insight user.
2. Check the status of RAMP:

```
/opt/sonus/ems/emsMgmt status
```

Understanding RAMP status from the command output

Parameter	Description
EMS VERSION	RAMP software version.
HA MODE	RAMP deployment model: • SA: standalone • GR: Geographical Redundancy
<service/process name> Running	Name of a service/process currently running in RAMP. If a service is not running, the status shows <service name> Not Running. In RAMP GR deployments, two instances of a service name indicates that the service is running on both the active and standby devices. Some processes run only on the active device, for example, Fault Management.
<service/process name> Not Running:	Name of a service/process currently not running in RAMP.
Configured State	Original state of the device when RAMP was configured. • SA: The device is originally configured as a standalone node. • Active: The device is originally configured as the active node in a cluster for redundancy. • Standby: The device is originally configured as the standby node in a cluster for redundancy.
Current State	Current state of the device. • SA: The device is currently acting as a standalone node. • Active: The device is currently acting as the active node in a cluster for redundancy. If the current state is different from the configured state, failover has occurred. Multiple occurrences of failover may restore a device to its configured state. • Standby: The device is currently acting as the standby node a cluster for redundancy. If the current state is different from the configured state, failover has occurred. Multiple occurrences of failover may restore a device to its configured state.

Check Deployment Status of Services in RAMP

Use the following procedure to show the deployment status of the services on the Ribbon Application Management Platform (RAMP) device. If you have deployed RAMP with redundancy, perform this procedure on the RAMP active device.

Start

1. SSH to the RAMP device as the admin user.
2. Change to the insight user:

```
sudo su - insight
```

3. Enter the following command:

```
/opt/sonus/ems/conf/serviceDeployed.sh
```

Change Time Zone on RAMP

The Ribbon Application Management Platform (RAMP) allows you to change the time zone. You can change the existing time zone of the RAMP server, the system clock, and the settings. The RAMP can accurately set and adjust time zones, ensuring that all time-sensitive operations, such as logging, scheduling, and reporting, are synchronized correctly. Proper time zone configuration is essential for maintaining the consistency and reliability of data across different geographical locations. By following the below steps, you can ensure that your RAMP setup is correctly aligned with your operational requirements, enhancing both efficiency and accuracy in your application management processes.

Perform the following procedure to change the time zone:

Start

1. Stop the RAMP:
 - a. Log on to the RAMP as an `insight` user. For more information, refer to [Log onto the RAMP CLI](#).
 - b. Stop the RAMP:

```
/opt/sonus/ems/emsMgmt stop
```

2. To change the time zone, run the following command as `root` user:

```
timedatectl set-timezone <timeZone>
```

Example Output:

```
[2024-05-16 16:00:04 root@RAMP2403: /home/admin ]# timedatectl set-timezone Asia/Irkutsk
```

3. Reboot the RAMP:


```
reboot
```

4. You can verify if the timezone has been updated by running `timedatectl` command:

Example Output:

```
timedatectl
          Local time: Thu 2024-05-16 16:15:16 IST
          Universal time: Thu 2024-05-16 10:45:16 UTC
            RTC time: Thu 2024-05-16 10:45:16
            Time zone: Asia/Kolkata (IST, +0530)
System clock synchronized: no
          NTP service: active
          RTC in local TZ: no
```

Deploy Optional Services on RAMP

In this section:

- [Deploy the Action Service](#)
- [Backup/ Restore/ Upgrade](#)
- [Deploy the EdgeView Service](#)
- [Deploy the Object Store Service](#)

The Ribbon Application Management Platform (RAMP) allows you to manage the SBC Edge, SBC 1000/2000, Edge 8000 series or EdgeMarc devices based on the services you deploy.

Deploy the Action Service

Action Service is developed to manage and support the actions applicable to the devices. Action service is responsible for the fulfilment of actions details on the RAMP GUI, handling user inputs, performing the action request and handling the action logs and status. In current release this feature is limited to Edge Marc device actions.

Use this procedure to deploy the action service. To control the network range of the new docker networks, refer to [How to Control the Network Range](#).

Note

Deploy the Action Service (ACS) before deploying the EdgeView Service on RAMP.

Start

1. SSH to RAMP as the `Insight` user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the `Insight` user.
2. Check the status of RAMP. For more information, refer to [Check RAMP Status](#).

3. Based on the output perform one of the following:
 - a. If the Action service status shows as "Running", no further action is required. Skip the remaining steps to deploy the Action service.
 - b. If Action service is not listed in the output of "emsMgmt status," deploy the Action service:
 - i. Access RAMP as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
 - ii. Change to root user:

```
sudo su -
```

- iii. Deploy the Action service:

```
/opt/action_service_config add
```

Backup/ Restore/ Upgrade

Backup:

The backup is created when the Action service is installed, and the backup tar file is included in the RAMP backup files. If the Action service is not installed, no backup will be created.

Restore:

During the restoration process, if the RAMP backup file contains action-service backup data and action-service is not installed on the setup where the restore is being performed:

- If action-service is not installed, it will be installed first and then restored.
- If action-service is already installed, it will be restored.

Upgrade:

In case of upgrade, if action-service is installed on the setup that is being upgraded then it will be upgraded. If action-service is not installed, then it will not be considered for upgrade.

Deploy the EdgeView Service

To manage SBC Edge, SBC 1000/2000, Edge 8000 series or EdgeMarc devices on the Ribbon Application Management Platform (RAMP), you must deploy the EdgeView service on RAMP. The EdgeView service is not deployed by default on RAMP. Use the following procedure to deploy the EdgeView Service on RAMP. This procedure begins by checking the status of the EdgeView service on RAMP with a step to deploy the EdgeView service if it is not already deployed. After installing the EdgeView Service, two additional docker interfaces are created on RAMP. To control the network range of the new docker networks, refer [How to Control the Network Range](#).

Start

1. SSH to RAMP as the `Insight` user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the `Insight` user.
2. Check the status of RAMP. For more information, refer to [Check RAMP Status](#).
3. Based on the output, perform one of the following:
 - If the "EdgeView" status shows as "Running", no further action is required. Skip the remaining steps to deploy the EdgeView service.

- If "EdgeView" is not listed in the output of "emsMgmt status," then deploy the EdgeView service:
 - i. Access [RAMP](#) as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing [RAMP](#) as the admin user.
 - ii. Change to root user:

```
sudo su -
```

- iii. Deploy the EdgeView service:

```
/opt/sonus/ems/conf/edge_view_config add
```

Deploy the Object Store Service

The Object Store service is currently optional. You can add it separately after [RAMP](#) is deployed. The Object Store Service includes the Apache Ozone S3 Object Store which is responsible to store the EdgeMarc device diagnostic snapshots and packet capture files. In this release, this service is applicable only for the EdgeMarc device. After installing the [Object service](#), two additional docker interfaces are created on [RAMP](#). To control network range of the new docker networks, refer [How to Control the Network Range](#).

Note

The Object Store service is only applicable for EdgeMarc services.

Start

1. SSH to [RAMP](#) as root user. Refer to [Log onto the RAMP CLI](#) for accessing [RAMP](#) as the root user.
2. Check the status of [RAMP](#). For more information, refer to [Check RAMP Status](#).
3. Based on the output, perform one of the following:
 - a. If the Object Store status shows as "Running", no further action is required. Skip the remaining steps to deploy the Object Store service.
 - b. If the Object Store is not listed in the output of "emsMgmt status", run the following steps to deploy the Object Store service:
 - i. Access [RAMP](#) as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing [RAMP](#) as the admin user.
 - ii. Change to root user:

```
sudo su -
```

- iii. Deploy the Object Store service:

```
/opt/object_store_service_config add
```

Download Files from Ribbon Support Portal

Use this procedure to download Ribbon product software bundles, patches and files.

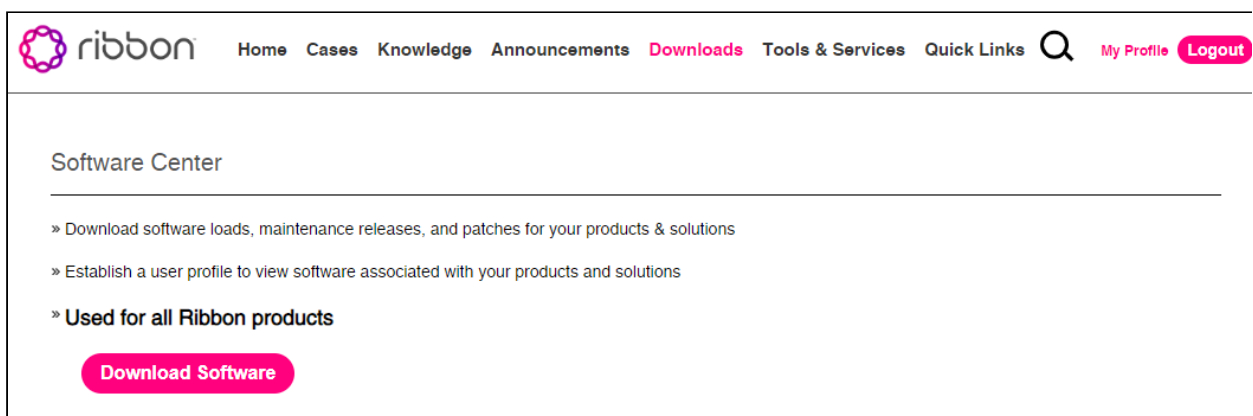
Start

1. Log in to the [Ribbon Support Portal](#) with your Ribbon-provided username and password.
2. From the menu bar, click **Downloads** to view the Software Center page.



3. From the Software Center page, click **Download Software**.

Before attempting to download product software, ensure your user profile is updated to view the software associated with your products and solutions.

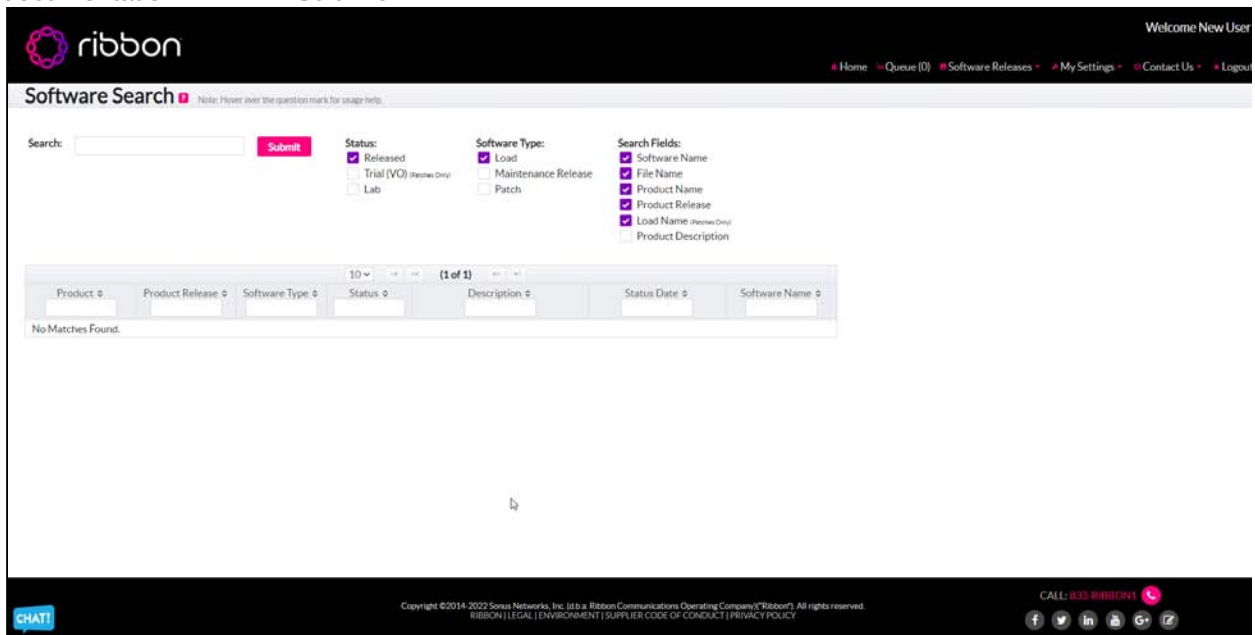


You are redirected to the Global Software Center.

4. From the menu bar, hover your cursor over **Software Releases** and then choose "Advanced Search."



5. In the **Search** field, enter the name or description of the desired product software bundle, patch or documentation and click **Submit**.



Note

You may select options for **Status**, **Software Type**, and **Search Fields** as required or leave them as default.

6. Double-click the product you want to download.
7. Select **Download** in the **Action** column for the file you wish to download.
8. The first time you download a software file, enter the end user name and address details. Click **Submit**.

9. Read the **End User License Agreement**. If you click **I Agree**, the software bundle/file/document downloads.

Export the RAMP Configuration Tables

In this section:

- [Schedule a Cron Job Automatically](#)
- [Export the Configuration Table Automatically](#)

Use the `configExport.sh` script to export the Ribbon Application Management Platform (RAMP) configuration tables in **Application Management** within **Insight Administration** and any other tables that store the RAMP configuration. The configuration tables are exported in CSV format. You can use the exported CSV files to perform audits against a "golden configuration" and compare lab configurations to production.

The CSV files are exported to the directory `/opt/sonus/ems/weblogic/sonusEms/data/configExport` in the RAMP.

One CSV file is generated for every table.

The list of exportable RAMP configuration tables is shown below.

Note

The following files are empty when exported:

- `config_app.device_group.csv`
- `config_license.licenseproperty.csv`

Exportable RAMP Configuration Tables

<code>config_license.licensehost.csv</code>
<code>config_license.licenseinfo.csv</code>
<code>pm.collection_cluster_map.csv</code>
<code>pm.collection_node_map.csv</code>
<code>pm.collection_profile.csv</code>
<code>pm.collection_profile_association.csv</code>

pm.pm_config_properties.csv
pm.pm_data_retention.csv
pm.pm_export_job.csv
pm.pm_export_loc_assoc.csv
pm.pm_export_location.csv
pm.pm_export_profile.csv
pm.pm_export_profile_cluster_map.csv
pm.pm_export_profile_node_map.csv
pm.pm_export_stats.csv
pm.pm_report_filters.csv
pm.pm_report_template.csv
pm.pm_reports.csv
pm.pm_thresholdcrossingevents.csv
pm.pm_thresholddescriptors.csv
fm.email_notification.csv
fm.email_notification_filter.csv
fm.en_alarm_information.csv
fm.filterprofiles.csv
fm.exporter_profile.csv
fm.sourceaddress.csv
fm.traptypefilter.csv
auth.access_control_association_t.csv

auth.user_config_t.csv
auth.service_privs_config_t.csv
auth.user_group_association_t.csv
auth.realm_config_t.csv
auth.tenant_config_t.csv
auth.user_group_config_t.csv
devmgmt.clustergroup.csv
devmgmt.clustergroupproperties.csv
devmgmt.clustergroupsnmpconfig.csv
devmgmt.resource_group.csv
devmgmt.resource_group_node.csv
devmgmt.resource_group_cluster.csv
devmgmt.resource_group_node_type.csv
devmgmt.resource_group_cluster_type.csv
config_common.config_properties.csv
config_app.emsconfiguration.csv
config_app.feature_permissions.csv
config_sys.systemconfig.csv

Schedule a Cron Job Automatically

Perform the following procedure to schedule a Cron Job to automatically export the tables at regular intervals.

Start

1. Log on to the RAMP as insight user.
2. Execute the following command:


```
crontab -e
```

3. Add the following string:

```
*/<Interval in minutes at which the configuration tables are exported from the  
RAMP> * * * * . /opt/sonus/ems/.profile; /opt/sonus/ems/conf/configExport.sh
```

Example with two-minute interval

```
*/2 * * * * . /opt/sonus/ems/.profile; /opt/sonus/ems/conf/configExport.sh
```

4. Save the changes.

Export the Configuration Table Automatically

Perform the following procedure to export the configuration tables manually.

Start

1. Navigate to the following directory in the RAMP:

```
/opt/sonus/ems/conf/
```

2. Run the `configExport.sh` script:

```
./configExport.sh
```

Sample output

```
Validating table list .....  
(success)  
config_license.licensehost found in database.  
..... (success)  
config_license.licenseinfo found in database.  
..... (success)  
config_license.licenseproperty found in database.  
..... (success)  
fm.email_notification found in database.  
..... (success)  
fm.email_notification_filter found in database.  
..... (success)  
fm.en_alarm_information found in database.  
..... (success)
```

```
fm.filterprofiles found in database.
..... (success)
fm.exporter_profile found in database.
..... (success)
fm.sourceaddress found in database.
..... (success)
fm.traptypefilter found in database.
..... (success)
auth.access_control_association_t found in database.
..... (success)
auth.user_config_t found in database.
..... (success)
auth.service_privs_config_t found in database.
..... (success)
auth.user_group_association_t found in database.
..... (success)
auth.realm_config_t found in database.
..... (success)
auth.tenant_config_t found in database.
..... (success)
auth.user_group_config_t found in database.
..... (success)
auth.role_config_t found in database.
..... (success)
auth.service_privs_association_t found in database.
..... (success)
auth.global_config_t found in database.
..... (success)
devmgmt.clustergroup found in database.
..... (success)
devmgmt.clustergroupproperties found in database.
..... (success)
devmgmt.clustergroupsnmpconfig found in database.
..... (success)
devmgmt.resource_group found in database.
..... (success)
devmgmt.resource_group_node found in database.
..... (success)
devmgmt.resource_group_cluster found in database.
..... (success)
devmgmt.resource_group_node_type found in database.
..... (success)
devmgmt.resource_group_cluster_type found in database.
..... (success)
pm.collection_cluster_map found in database.
..... (success)
pm.collection_node_map found in database.
..... (success)
pm.collection_profile found in database.
..... (success)
pm.collection_profile_association found in database.
..... (success)
pm.pm_config_properties found in database.
```

```

..... (success)
pm.pm_data_retention found in database.
..... (success)
pm.pm_export_job found in database.
..... (success)
pm.pm_export_loc_assoc found in database.
..... (success)
pm.pm_export_location found in database.
..... (success)
pm.pm_export_profile found in database.
..... (success)
pm.pm_export_profile_cluster_map found in database.
..... (success)
pm.pm_export_profile_node_map found in database.
..... (success)
pm.pm_export_stats found in database.
..... (success)
pm.pm_report_filters found in database.
..... (success)
pm.pm_report_template found in database.
..... (success)
pm.pm_reports found in database.
..... (success)
pm.pm_thresholdcrossingevents found in database.
..... (success)
pm.pm_thresholddescriptors found in database.
..... (ok)
Creating new export directory ..... (ok)
-----

.....
Exporting LM DB tables
.....
-----

..... Exporting
config_license.licensehost ..... (ok)
Exporting config_license.licenseinfo ..... (ok)
Exporting config_license.licenseproperty ..... (ok)
-----

.....
Exporting LM DB tables
.....
-----

..... Exporting
pm.collection_cluster_map ..... (ok)
Exporting pm.collection_node_map ..... (ok)
Exporting pm.collection_profile ..... (ok)
Exporting pm.collection_profile_association ..... (ok)
Exporting pm.pm_config_properties ..... (ok)
Exporting pm.pm_data_retention ..... (ok)
Exporting pm.pm_export_job ..... (ok)
Exporting pm.pm_export_loc_assoc ..... (ok)
Exporting pm.pm_export_location ..... (ok)
Exporting pm.pm_export_profile ..... (ok)

```

```

Exporting pm.pm_export_profile_cluster_map ..... (ok)
Exporting pm.pm_export_profile_node_map ..... (ok)
Exporting pm.pm_export_stats ..... (ok)
Exporting pm.pm_report_filters ..... (ok)
Exporting pm.pm_report_template ..... (ok)
Exporting pm.pm_reports ..... (ok)
Exporting pm.pm_thresholdcrossingevents ..... (ok)
Exporting pm.pm_thresholddescriptors ..... (ok)
-----
.....
Exporting FM DB tables
-----
.....
Exporting
fm.email_notification ..... (ok)
Exporting fm.email_notification_filter ..... (ok)
Exporting fm.en_alarm_information ..... (ok)
Exporting fm.filterprofiles ..... (ok)
Exporting fm.exporter_profile ..... (ok)
Exporting fm.sourceaddress ..... (ok)
Exporting fm.traptypefilter ..... (ok)
-----
.....
Exporting AUTH DB tables
-----
.....
Exporting
auth.access_control_association_t ..... (ok)
Exporting auth.user_config_t ..... (ok)
Exporting auth.service_privs_config_t ..... (ok)
Exporting auth.user_group_association_t ..... (ok)
Exporting auth.realm_config_t ..... (ok)
Exporting auth.tenant_config_t ..... (ok)
Exporting auth.user_group_config_t ..... (ok)
Exporting auth.role_config_t ..... (ok)
Exporting auth.service_privs_association_t ..... (ok)
Exporting auth.global_config_t ..... (ok)
-----
.....
Exporting DM DB tables
-----
.....
Exporting
devmgmt.clustergroup ..... (ok)
Exporting devmgmt.clustergroupproperties ..... (ok)
Exporting devmgmt.clustergroupsnmpconfig ..... (ok)
Exporting devmgmt.resource_group ..... (ok)
Exporting devmgmt.resource_group_node ..... (ok)
Exporting devmgmt.resource_group_cluster ..... (ok)
Exporting devmgmt.resource_group_node_type ..... (ok)
Exporting devmgmt.resource_group_cluster_type ..... (ok)
-----
.....

```

```

Exporting Insight DB tables
.....
-----
..... Exporting
config_common.config_properties ..... (ok)
Exporting config_app.device_group ..... (ok)
Exporting config_app.emsconfiguration ..... (ok)
Exporting config_app.feature_permissions ..... (ok)
Exporting config_sys.systemconfig ..... (ok)
EXPORT COMPLETE

```

Example exported configuration file

```

-bash-4.4$ cat pm.collection_profile.csv
profile_id,profile_name,device_type,interface,default_gen_freq,default_coll_freq,d
efault_profile
1,Default DSC SFTP Profile,DSC,SFTP,,5,t
34,Default SLB SFTP Profile,SLB,SFTP,5,5,t
62,Default PSX6000 SFTP Profile,PSX6000,SFTP,5,5,t
172,Default DSI SNMP Profile,DSI,SNMP,,5,t
175,Default GSX9000 SNMP Profile,GSX9000,SNMP,,5,t
205,Default GSX9000 SFTP Profile,GSX9000,SFTP,5,5,t
235,Default INSIGHT SFTP Profile,INSIGHT,SFTP,,5,t
239,Default EDGE SFTP Profile,EDGE,SFTP,,5,t
243,Default SGX4000 SNMP Profile,SGX4000,SNMP,,5,t
258,Default SBX5K SFTP Profile,SBX5K,SFTP,5,5,t
1741,Sample SNMP profile,PSX6000,SNMP,,5,f
-bash-4.4$

```

All columns in the configuration tables are exported. The first line in the file contains a header listing the names of the table's columns.

Every subsequent line in the file corresponds to a row in the table.

For each export, the audit files are overwritten to prevent filling up the disk partition with these files.

You can run the script as a Cron Job and set the frequency and time of running the Cron Job.

The log file for the `configExport.sh` command is `configExport.log`. It is located in the RAMP at `/opt/sonus/ems/logs`.

Install PSX Manager on RAMP

Use this procedure to install the PSX Manager on Ribbon Application Management Platform (RAMP).

Start

1. SSH to RAMP as the insight user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the insight user.
2. Verify if the PSX Manager version is the latest version:

```
rpm -qa | grep SONSpssx
```

Note

If the PSX Manager version is not the latest then download the respective PSX Manager GUI TAR file (SSGUI_<Version>_RHEL.tar) and execute upgrade steps from Step 3 onwards.

3. Stop RAMP:

```
/opt/sonus/ems/emsMgmt stop
```

4. Change to root user.

5. If the /opt/sonus/install/ directory is not available, create the directory:

```
mkdir -p /opt/sonus/install/
```

6. Download the SSGUI_V<version>_RHEL.tar file from the Ribbon Support Portal to the local system.

7. Copy the SSGUI_V<version>_RHEL.tar file from the local system to the /opt/sonus/install/ directory on RAMP.

8. Navigate to /opt/sonus/install/ directory:

```
cd /opt/sonus/install/
```

9. Untar the SSGUI_V<version>_RHEL.tar file:

```
tar -xvf SSGUI_V<version>RHEL.tar
```

10. Navigate to the /opt/sonus/install/SSGUI directory :

```
cd /opt/sonus/install/SSGUI
```

11. Change the permissions of GuiClient.sh to executable:

```
chmod 777 GuiClient.sh
```

12. Enter the following command:

```
./GuiClient.sh
```

- If an older version of PSX Manager does not exist, the following output displays.

```
...
```

```
package SONSPsx is not installed
```

```
Installing SONSPsx.
```

```
Preparing... ##### [100%]
```

```
Updating / installing...
```

```
 1:SONSPsx-<version> ##### [100%]
```

- If a prior version of PSX Manager exists, a confirmation message to remove the existing version displays.

```
/opt/sonus/ems/weblogic/insight/deployments/insight.ear/emsGui.war/external
SONSPsx-V13.00.00-R000.x86_64
```

```
Version V<version> already exists. It must be removed to proceed.
```

```
Remove the existing version? (default: N) [y|Y,n|N]:
```

- i. Enter **y** to uninstall the prior version and install the latest version of PSX Manager. The following message displays.

```
Removing SONSPsx.
```

```
Installing SONSPsx.
```

```
Preparing... ##### [100%]
```

```
]
```

```
Updating / installing...
```

```
 1:SONSPsx-<version> ##### [100%]
```

```
]
```

13. Verify that the `SONSPsx` package is installed:

```
rpm -qa | grep SONSPsx
```

14. Change to the insight user.
15. Start RAMP:

```
/opt/sonus/ems/emsMgmt start
```

16. Log on to the RAMP GUI.
17. Check [PSX Manager version compatibility with RAMP](#).
18. Click **Reload** to integrate the new PSX Manager version to RAMP.

Managing Accounts and Passwords

In this section:

- [Manage RAMP Account Names and Passwords](#)

- [Change Linux Admin User Password on RAMP Standalone](#)
- [Change Linux Admin User Password on RAMP GR](#)
- [Change Linux Insight User Password on RAMP Standalone](#)
- [Change Linux Insight User Password on RAMP GR](#)
- [Change RAMP Keystore Password](#)
- [Change the Insight Database User Password](#)
- [Change the Insight Postgres DB User Password](#)
- [Change the admin Password for the Insight Agent](#)
- [Change the Insight \(RAMP\) GUI Admin User Password](#)
- [Change the restuser Password for the Insight \(RAMP\) REST API](#)
- [Reset RAMP GUI Admin Password](#)
- [Unlock Database User dbimpl](#)
- [Generate a Master Key to Encrypt RAMP Passwords](#)
- [Manage User Accounts](#)
 - [Unlock a User Account](#)
 - [Set User Permissions](#)
 - [Modify Passwords](#)
 - [Modify User Session Timeout Interval](#)
 - [Limit the Maximum Number of Login Sessions](#)
 - [Configure User Account Lock Settings](#)
 - [Enable Users to Create Cron Jobs](#)
 - [Enable Users to Create 'at' Jobs](#)
- [Establish Passwordless Connection from an External Server to RAMP](#)
- [Establish RAMP CNF Active-Standby Instance Passwordless Connection](#)
- [Change the GRUB Password](#)

Manage RAMP Account Names and Passwords

In this section:

- [RAMP Application-Specific Accounts](#)
- [RAMP Linux Accounts](#)
- [RAMP Database Accounts](#)
- [Insight Agent Account](#)
- [RAMP Keystore Password](#)

Related articles:

- [Change Linux Admin User Password on RAMP Standalone](#)
- [Change Linux Admin User Password on RAMP GR](#)
- [Change Linux Insight User Password on RAMP Standalone](#)
- [Change Linux Insight User Password on RAMP GR](#)
- [Change RAMP Keystore Password](#)
- [Change the Insight Database User Password](#)
- [Change the Insight Postgres DB User Password](#)
- [Change the admin Password for the Insight Agent](#)
- [Change the Insight \(RAMP\) GUI Admin User Password](#)
- [Change the restuser Password for the Insight \(RAMP\) REST API](#)

- [Reset RAMP GUI Admin Password](#)
- [Unlock Database User dbimpl](#)
- [Generate a Master Key to Encrypt RAMP Passwords](#)
- [Managing RAMP Users and Accounts \(Security Best Practice\)](#)

This section covers account names and passwords associated with Ribbon Application Management Platform (RAMP).

The RAMP default accounts include those associated with the Linux and those associated with the underlying Insight database.

Note

All the user accounts listed in this section are mandatory. You cannot disable or remove any of these users.

RAMP Application-Specific Accounts

This section provides list of accounts name and passwords associated with the RAMP application.

Account name	User ID	Default password	How to change the password?
RAMP GUI account	admin	admin	Change User Password
RAMP REST API account	restuser	sonus123	Device REST Credentials

RAMP Linux Accounts

Account name	User ID	Default password		How to change the password?	Usage	Password expiry
		non-cloud (KVM/VMWare)	cloud (Openstack/AWS/Azure)			
Admin user	admin	admin	admin	- To change admin password on RAMP standalone, refer to Change Linux Admin User Password on RAMP Standalone. - To change admin password on RAMP GR, refer to Change Linux Admin User Password on RAMP GR.	The super user account used for all administrative activities. This account has sudo permissions.	90 days Note The admin user account password expiry does not apply to RAMP CNF.

Account name	User ID	Default password		How to change the password?	Usage	Password expiry
		non-cloud (KVM/VMWare)	cloud (Openstack/AWS/Azure)			
Insight	insight	insight	insight	- To change insight password on RAMP standalone, refer to Change Linux Insight User Password on RAMP Standalone. - To change insight password on RAMP GR, refer to Change Linux Insight User Password on RAMP GR.	The primary account used for all non-administrative tasks including maintenance activities.	never
Postgres	postgres	N/A	N/A	Change the Insight Postgres DB User Password	Manage the Postgres database running on RAMP.	never

Password Aging

Perform the following procedure to modify the password aging:

As a `root` user and modify `maximum password aging days` parameter:

```
chage -M <MAX_PASS_DAYS> <username>
```

An example to change the password expiry to 180 days:

Example

```
chage -M 180 admin
```

RAMP Database Accounts

Account name	User ID	Default password (weak passwords only)	How to change the password?	Usage
Data base User	dbimpl	dbimpl123	Change the Insight Database User Password	The insight database account used for connecting to the database.

Insight Agent Account

Account Name	User ID	Default password (weak password only)	How to change the password?	Usage
Insight Agent Admin User	admin	admin	Change the admin Password for the Insight Agent	All configuration operations and retrieval of data from the Agent. This includes PM statistics collection and configuring the PM collection interval and the RAMP IP addresses which will be managing the Agent.

RAMP Keystore Password

Account name	User ID	Default password	How to change the password?	Usage
N/A	N/A	sonusems	Change RAMP Keystore Password	Secure the keystore which contains the certificate used by RAMP for all clients to RAMP HTTPS/TLS connections.

Change Linux Admin User Password on RAMP Standalone

Use this procedure to change the admin passwords on Ribbon Application Management Platform (RAMP) standalone. To change the admin password on RAMP GR, refer to [Change Linux Admin User Password on RAMP GR](#).

Password Criteria

The password must meet the following criteria:

- Start with an upper case or lower case letter.
- At least 16 characters.
- Contain characters from each of the following four categories:
 - lowercase letters
 - uppercase letters
 - numerals
 - _ or #

Start

1. SSH to RAMP as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command:

```
/opt/sonus/ems/conf/changePassword.py
```

The following prompt displays:

```
EMS Password changing tool
-----
This Script is able to change following EMS (Standalone|GR|HA) accounts password
  1. Linux Insight User (insight)
  2. Linux Admin User (admin)
  3. Insight DB User (dbimpl)
  4. Insight Postgres DB User (postgres)
  5. Insight Agent (admin)
  6. Insight GUI Admin User (admin)
  7. Insight REST API user (restuser)

Usage:-
  changePassword -o <option_number>
-----
(Enter command or ?) :
```

4. Enter the following command:

```
changePassword -o 2
```

The following prompt displays:

```
Please enter new password:
```

5. Enter the new password. The following prompt is displayed:

```
Please re-enter new password:
```

6. Enter the new password again. The following output displays.

```
2020-07-30 10:59:29.237386 changePassword :
    Linux ADMIN password change in progress
2020-07-30 10:59:29.252160 changeLinuxAdminPassword :
    Password changing in progress for Linux 'admin'
2020-07-30 10:59:29.701414 changeLinuxAccountHelper :
    Password changed for 'admin' user on local EMS
```

7. Exit the `changePassword.py` script:

```
exit
```

Change Linux Admin User Password on RAMP GR

Use this procedure to change the admin passwords on RAMP GR. To change admin password on RAMP standalone, refer to [Change Linux Admin User Password on RAMP Standalone](#).

Password Criteria

The password must meet the following criteria:

- Start with an upper case or lower case letter.
- At least 16 characters.
- Contain characters from each of the following four categories:
 - lowercase letters
 - uppercase letters
 - numerals
 - _ or #

Start

1. SSH to RAMP as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command:

```
/opt/sonus/ems/conf/changePassword.py
```

The following prompt displays:

```
EMS Password changing tool
-----
This Script is able to change following EMS (Standalone|GR|HA) accounts password
  1. Linux Insight User (insight)
  2. Linux Admin User (admin)
  3. Insight DB User (dbimpl)
```

```

4. Insight Postgres DB User (postgres)
5. Insight Agent (admin)
6. Insight GUI Admin User (admin)
7. Insight REST API user (restuser)

Usage:-
    changePassword -o <option_number>
-----
(Enter command or ?) :

```

4. Enter the following command:

```
changePassword -o 2
```

The following prompt displays:

```
Please enter new password:
```

5. Enter the new password. The following prompt displays:

```
Please re-enter new password:
```

6. Enter the new password again. The following output is displayed. At the end of the output, you are prompted to enter the current password of the remote machine.

```

Please enter new password:
Please re-enter new password:
2020-07-27 10:47:32.138682 changePassword :
Linux ADMIN password change in progress
2020-07-27 10:47:32.144469 changeLinuxAdminPassword :
Password changing in progress for Linux 'admin'
2020-07-27 10:47:32.498220 changeLinuxAccountHelper :
Password changed for 'admin' user on local EMS

```

7. Exit the `changePassword.py` script:

```
exit
```

Change Linux Insight User Password on RAMP Standalone

This procedure covers changing the Linux insight password on Ribbon Application Management Platform (RAMP) standalone.

To change the Linux insight password on RAMP GR, refer to [Change Linux Insight User Password on RAMP GR](#).

Password Criteria

The password must meet the following criteria:

- Start with an upper case or lower case letter.

- At least 16 characters.
- Contain characters from each of the following four categories:
 - lowercase letters
 - uppercase letters
 - numerals
 - _ or #

Start

1. SSH to **RAMP** as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command:

```
/opt/sonus/ems/conf/changePassword.py
```

The following prompt displays:

```
EMS Password changing tool
-----
This Script is able to change following EMS (Standalone|GR|HA) accounts password
  1. Linux Insight User (insight)
  2. Linux Admin User (admin)
  3. Insight DB User (dbimpl)
  4. Insight Postgres DB User (postgres)
  5. Insight Agent (admin)
  6. Insight GUI Admin User (admin)
  7. Insight REST API user (restuser)

Usage:-
  changePassword -o <option_number>
-----
(Enter command or ?) :
```

4. Enter the following command:

```
changePassword -o 1
```

The following prompt is displayed:

```
Please enter new password:
```

5. Enter the new password.
The following prompt is displayed:

```
Please re-enter new password:
```

6. Enter the new password again. The following output is displayed.


```

2020-07-27 01:47:58.894646 changePassword :
    Linux INSIGHT password change in progress, may take 2 - 5 minutes
    depending on EMS type
2020-07-27 01:48:19.575101 changeInsightPasswordHelper :
    Password changed for Insight user
2020-07-27 01:48:19.678126 changePassword :
    Linux INSIGHT Password Change Successful!
(Enter command or ?) :

```

7. Exit the `changePassword.py` script:

```
exit
```

Change Linux Insight User Password on RAMP GR

This procedure covers changing the Linux insight password on Ribbon Application Management Platform (RAMP) GR.

To change the Linux insight password on RAMP standalone, refer to [Change Linux Insight User Password on RAMP Standalone](#).

Password criteria

The password must meet the following criteria:

- Start with an upper case or lower case letter.
- At least 16 characters.
- Contain characters from each of the following four categories:
 - lowercase letters
 - uppercase letters
 - numerals
 - _ or #

Start

1. SSH to RAMP as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command:

```
/opt/sonus/ems/conf/changePassword.py
```

The following prompt displays:

```

EMS Password changing tool
-----
This Script is able to change following EMS (Standalone|GR|HA) accounts password
    1. Linux Insight User (insight)
    2. Linux Admin User (admin)

```

```

3. Insight DB User (dbimpl)
4. Insight Postgres DB User (postgres)
5. Insight Agent (admin)
6. Insight GUI Admin User (admin)
7. Insight REST API user (restuser)

Usage:-
    changePassword -o <option_number>
-----
(Enter command or ?) :
```

4. Execute the following command:

```
changePassword -o 1
```

The following prompt is displayed:

```
Please enter new password:
```

5. Enter the new password.
The following prompt is displayed:

```
Please re-enter new password:
```

6. Enter the new password again. The following output is displayed.

```

2020-07-27 11:06:09.409630 changePassword :
    Linux INSIGHT password change in progress, may take 2 - 5 minutes
    depending on EMS type
2020-07-27 11:06:09.411459 changeInsightPassword :
    This is a GR EMS - peer EMS Linux 'insight' user will be updated too
```

7. Exit the `changePassword.py` script:

```
exit
```

Change RAMP Keystore Password

The Ribbon Application Management Platform (RAMP) certificate used for the TLS connections is stored in the keystore.

This section covers how to change the RAMP keystore password with the `changeKeystorePassword.sh` script. For the default password, refer to [Manage RAMP Account Names and Passwords](#).

Perform this procedure only after obtaining and importing your own SSL certificate. Refer to [Secure Login to the RAMP GUI](#).

Note

You cannot perform this procedure using the demo site certificate that comes with the RAMP.

Prerequisites

The password can contain any character.

Start

1. SSH to RAMP as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command:

```
/opt/sonus/ems/conf/changeKeystorePassword.sh
```

The following prompt appears:

```
Please enter the current EMS keystore password:
```

4. Enter the password.
The following prompt appears:

```
Please enter the private key alias:
```

5. Enter the private key alias.

Note

If `genCertRequest` script is used to generate the private key, then the private key alias is `insight`. Refer to [Secure Login to the RAMP GUI](#).

The following prompt appears:

```
Please enter the private key password:
```

6. Enter the private key password.

The following prompt appears:

```
Please enter new password:
```

7. Enter the new RAMP keystore password.
8. When prompted, re-enter the password.
The script runs to completion.

Change the Insight Database User Password

Use this procedure to change the database user (dbimpl) password for the Ribbon Application Management Platform (RAMP) database.

For RAMP GR, enter this command on the RAMP active node.

Password Criteria

The password must meet the following criteria:

- Start with an upper case or lower case letter.
- At least 8 characters.
- Contain characters from each of the following four categories:
 - lowercase letters
 - uppercase letters
 - numerals
 - _ or #

For example, "Ribbon#12_3"

Start

1. SSH to RAMP as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command:

```
/opt/sonus/ems/conf/changePassword.py
```

The following prompt displays:

```
EMS Password changing tool
-----
This Script is able to change following EMS (Standalone|GR|HA) accounts password
  1. Linux Insight User (insight)
  2. Linux Admin User (admin)
  3. Insight DB User (dbimpl)
  4. Insight Postgres DB User (postgres)
  5. Insight Agent (admin)
  6. Insight GUI Admin User (admin)
  7. Insight REST API user (restuser)

Usage:-
  changePassword -o <option_number>
-----
(Enter command or ?) :
```

4. Enter the following command:

```
changePassword -o 3
```

The following prompt displays:

```
Please enter new password:
```

5. Enter the new password. The following prompt displays:

Please re-enter new password:

6. Enter the new password again. The following output displays.

```
2020-07-30 11:32:43.578122 changePassword :
    Insight DB (dbimpl) password change in progress, may take up to 10 minutes
    as EMS will be rebooted
2020-07-30 11:32:44.487649 changeInsightDBPassword :
    Changing DBIMPL password
2020-07-30 11:32:44.699947 changeInsightDBPasswordHelper :
    Changing password for DB user, please wait
2020-07-30 11:32:46.493564 changeInsightDBPassword :
    Insight DB user password changed
2020-07-30 11:32:46.596132 changePassword :
    Insight DB (dbimpl) Password Change Successful!
(Enter command or ?) :
```

7. Exit the `changePassword.py` script:

```
exit
```

Validate password change

1. SSH to [RAMP](#) as the admin user.
2. Enter the following command:

```
su - postgres
```

3. Enter the password.
4. Execute the following command:

```
psql -U dbimpl -d dbimpl -h <the IP address of RAMP> -p 5432
```

The following is an example:

```
psql -U dbimpl -d dbimpl -h 10.54.58.189 -p 5432
```

The following message displays:

```
Password for user dbimpl:
```

5. Enter the password. The following message displays:

```
psql (12.1)
Type "help" for help.

dbimpl=>
```

Change the Insight Postgres DB User Password

Use this procedure to change the password for the postgres database user on Ribbon Application Management Platform (RAMP) standalone or GR.

Password criteria

The password must meet the following criteria:

- Start with an upper case or lower case letter.
- At least 8 characters.
- Contain characters from each of the following four categories:
 - lowercase letters
 - uppercase letters
 - numerals
 - _ or #

For example, "Ribbon#12_3"

Start

1. SSH to RAMP as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command:

```
/opt/sonus/ems/conf/changePassword.py
```

The following prompt displays:

```
EMS Password changing tool
-----
This Script is able to change following EMS (Standalone|GR|HA) accounts password
  1. Linux Insight User (insight)
  2. Linux Admin User (admin)
  3. Insight DB User (dbimpl)
  4. Insight Postgres DB User (postgres)
  5. Insight Agent (admin)
  6. Insight GUI Admin User (admin)
  7. Insight REST API user (restuser)

Usage:-
    changePassword -o <option_number>
-----
(Enter command or ?) :
```

4. Enter the following command:

```
changePassword -o 4
```

The following prompt displays:

Please enter **new** password:

5. Enter the new password again. The following prompt displays:

Please re-enter **new** password:

6. Enter the new password again.
The following output displays.

```
2020-07-31 02:13:11.519155 changePassword :
      Postgres password change in progress
2020-07-31 02:14:09.217555 changePostgresPassword :
      Changing password for Postgres DB.
(Enter command or ?) :
```

7. Exit the `changePassword.py` script:

```
exit
```

Change the admin Password for the Insight Agent

For Ribbon Application Management Platform (RAMP) GR, change the password on the active node.

When you change the password for Linux Agent (admin) password on the **RAMP** active node, the password on the **RAMP** node also changes.

Password criteria

The password must meet the following criteria:

- Start with an upper case or lower case letter.
- At least 8 characters.
- Contain characters from each of the following four categories:
 - lowercase letters
 - uppercase letters
 - numerals
 - `_` or `#`

For example, "Ribbon#12_3"

Start

1. SSH to **RAMP** as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command:

```
/opt/sonus/ems/conf/changePassword.py
```

The following prompt displays:

```
EMS Password changing tool
-----
This Script is able to change following EMS (Standalone|GR|HA) accounts password
  1. Linux Insight User (insight)
  2. Linux Admin User (admin)
  3. Insight DB User (dbimpl)
  4. Insight Postgres DB User (postgres)
  5. Insight Agent (admin)
  6. Insight GUI Admin User (admin)
  7. Insight REST API user (restuser)

Usage:-
  changePassword -o <option_number>
-----
(Enter command or ?) :
```

4. Enter the following command:

```
changePassword -o 5
```

The following prompt is displayed:

```
Enter current password:
```

5. Enter the current password. The following prompt displays:

```
Please enter new password:
```

6. Enter the current password. The following prompt is displayed:

```
Please re-enter new password:
```

7. Enter the new password again.

The following output displays for RAMP standalone.

```
2020-07-31 04:03:07.465399 changePassword :
    Agent ADMIN password change in progress, may take 2 - 4 minutes depending
on EMS type
2020-07-31 04:03:07.481202 loginToAgent :
    Trying logon admin, attempt 0
2020-07-31 04:03:08.502273 changeAgentPasswordHelper :
    Logon success, now changing the password
2020-07-31 04:03:10.164652 changeAgentPasswordHelper :
    Password change successful
2020-07-31 04:04:10.164652 changePassword :
    Agent ADMIN Password Change Successful!
```



```
(Enter command or ?)
```

The following output displays for RAMP GR.

```
2020-07-31 02:28:37.663837 changePassword :
    Agent ADMIN password change in progress, may take 2 - 4 minutes depending
on EMS type
2020-07-31 02:28:37.669726 loginToAgent :
    Trying logon admin, attempt 0
2020-07-31 02:28:38.673715 changeAgentPasswordHelper :
    Logon success, now changing the password
2020-07-31 02:28:40.348156 changeAgentPasswordHelper :
    Password change successful
2020-07-31 02:28:40.652218 changeAgentPassword :
    This is a EMS RD cluster - updating remote agent's password on
10.54.58.174
2020-07-31 02:28:40.654397 loginToAgent :
    Trying to connect 10.54.58.174
2020-07-31 02:28:41.903192 loginToAgent :
    Trying logon admin, attempt 0
2020-07-31 02:28:43.135871 changeAgentPasswordHelper :
    Logon success, now changing the password
2020-07-31 02:28:44.828762 changeAgentPasswordHelper :
    Password change successful
2020-07-31 02:28:45.333281 changePassword :
    Agent ADMIN Password Change Successful!
(Enter command or ?) :
```

8. Exit the `changePassword.py` script:

```
exit
```

Change the Insight (RAMP) GUI Admin User Password

Follow this procedure to change the Ribbon Application Management Platform (RAMP) GUI admin user password.

For RAMP GR, enter this command on the RAMP active node.

Password Criteria

The password must meet the following criteria:

- Start with an upper case or lower case letter.
- At least 8 characters.
- Contain characters from each of the following four categories:
 - lowercase letters
 - uppercase letters
 - numerals
 - `_` or `#`

For example, "Ribbon#12_3"

Start

1. SSH to RAMP as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command:

```
/opt/sonus/ems/conf/changePassword.py
```

The following prompt displays:

```
EMS Password changing tool
-----
This Script is able to change following EMS (Standalone|GR|HA) accounts password
  1. Linux Insight User (insight)
  2. Linux Admin User (admin)
  3. Insight DB User (dbimpl)
  4. Insight Postgres DB User (postgres)
  5. Insight Agent (admin)
  6. Insight GUI Admin User (admin)
  7. Insight REST API user (restuser)

Usage:-
    changePassword -o <option_number>
-----
(Enter command or ?) :
```

4. Enter the following command:

```
changePassword -o 6
```

The following prompt is displayed:

```
Enter current password:
```

5. Enter the current password. The following prompt is displays:

```
Please enter new password:
```

6. Enter the current password. The following prompt displays:

```
Please re-enter new password:
```

7. Enter the new password again. The following output is displayed.

```
2018-08-06 07:56:25.116092 changePassword :
    GUI ADMIN password change in progress
```

```

2018-08-06 07:56:25.316712 guiAndRestUserPasswordHelper :
    Just a debug line to say prompt found
2018-08-06 07:56:28.256228 guiAndRestUserPasswordHelper :
    Password changed for GUI 'admin' user
2018-08-06 07:56:28.358615 changePassword :
    GUI ADMIN Password Change Successful!
(Enter command or ?) :

```

8. Exit the `changePassword.py` script:

```
exit
```

Change the restuser Password for the Insight (RAMP) REST API

Use this procedure to change the REST API user password on Ribbon Application Management Platform (RAMP).

For RAMP GR, enter this command on the RAMP active node.

Password Criteria

The password must meet the following criteria:

- Start with an upper case or lower case letter.
- At least 8 characters.
- Contain characters from each of the following four categories:
 - lowercase letters
 - uppercase letters
 - numerals
 - _ or #

For example, "Ribbon#12_3"

Start

1. SSH to RAMP as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command:

```
/opt/sonus/ems/conf/changePassword.py
```

The following prompt displays:

```

EMS Password changing tool
-----
This Script is able to change following EMS (Standalone|GR|HA) accounts password
  1. Linux Insight User (insight)
  2. Linux Admin User (admin)

```

3. Insight DB User (dbimpl)
4. Insight Postgres DB User (postgres)
5. Insight Agent (admin)
6. Insight GUI Admin User (admin)
7. Insight REST API user (restuser)

Usage:-

```
changePassword -o <option_number>
```

(Enter command or ?) :

4. Enter the following command:

```
changePassword -o 7
```

The following prompt is displayed:

Enter current password:

5. Enter the current password. The following prompt is displayed:

Please enter **new** password:

6. Enter the current password. The following prompt is displayed:

Please re-enter **new** password:

7. Enter the new password again. The following output is displayed.

```
2020-07-31 04:25:33.963660 changePassword :
    RestUser password change in progress
2020-07-31 04:25:34.282819 guiAndRestUserPasswordHelper :
    Just a debug line to say prompt found
2020-07-31 04:25:37.054207 guiAndRestUserPasswordHelper :
    Password changed for REST 'restuser' user
2020-07-31 04:25:37.155938 changePassword :
    RestUser Password Change Successful! The system will need to be re-started
```

8. Exit the `changePassword.py` script:

```
exit
```

Reset RAMP GUI Admin Password

Use the procedure on this page to reset the Ribbon Application Management Platform (RAMP) GUI password.

On a Geographically Redundant (GR) RAMP, perform this procedure on the active node:

If you know your password and want to change it, refer to [Change the Insight \(RAMP\) GUI Admin User Password](#).

Start

1. SSH to the RAMP as the `admin` user. Refer to [Log onto the RAMP CLI](#) to access the RAMP as the `admin` user.
2. Change to root user:

```
sudo su -
```

3. Reset the admin password:

```
/opt/sonus/auth/serviceScript.sh reset_admin_password
```

The following prompt is displayed:

```
Invoking password creation tool...  
Please enter the password:
```

Output:

```
Updating database to set new password for admin user...  
Password updated successfully! Please restart Auth service immediately to make the  
new password in effect.
```

4. Change to insight user:

```
sudo su - insight
```

5. Stop RAMP:

```
/opt/sonus/ems/emsMgmt stop
```

6. Start RAMP:

```
/opt/sonus/ems/emsMgmt start
```

The RAMP GUI password is reset. You can now log on to the RAMP GUI with the new password.

Unlock Database User dbimpl

If the database user (dbimpl) is locked out of the database, to unlock the database user (dbimpl):

1. SSH to RAMP as the admin user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command:

```
/opt/sonus/ems/conf/unlockDbimplUser.sh
```

Generate a Master Key to Encrypt RAMP Passwords

After Ribbon Application Management Platform (RAMP) installation, RAMP uses a default master key to encrypt all passwords. Use the following procedure to generate a new master key. When generating the master key you must specify a key size (128 bits or 256 bits). Once the new master key is generated, all RAMP passwords are decrypted using the old key, and then re-encrypted using the new master key.

Access the RAMP GUI at least once before generating a new master key to encrypt passwords with the initial key.

To generate a new master-key (for RAMP geo-redundant (GR) deployments, perform this procedure on the active node):

1. Log into RAMP as the `insight` user. Refer to [Log onto the RAMP CLI](#) for information.
2. Navigate to the following directory in the RAMP:

```
cd /opt/rbbn/ems/conf/
```

3. Perform one of the following depending on the key size you want:
 - To generate a master-key using a 128-bit key size, issue the following:

```
./masterKeyGenerator.sh AES_128
```

- To generate a master key using a 256-bit key size, issue the following:

```
./masterKeyGenerator.sh AES_256
```

If you do not specify a key size, then the new master key is generated using the default key size of 256 bits (AES_256).

The following output displays after successfully generating the master key and re-encrypting the existing passwords:

```
Keystore file change successfully.
```

RAMP restarts after the master key change. After the master key is generated and the existing passwords are encrypted, all RAMP credentials remain the same.

Manage User Accounts

In this section:

- [Unlock a User Account](#)
- [Set User Permissions](#)
- [Modify Passwords](#)
- [Modify User Session Timeout Interval](#)
- [Limit the Maximum Number of Login Sessions](#)
- [Configure User Account Lock Settings](#)
- [Enable Users to Create Cron Jobs](#)
- [Enable Users to Create 'at' Jobs](#)

Unlock a User Account

To maintain system security, a Ribbon Application Management Platform (RAMP) user account locks under certain circumstances.

Perform the following procedure if the account is locked due to user inactivity:

1. Log on as `admin` user.
2. Change to `root` user.
3. Use the following command:

```
#faillock --user <locked user> --reset
```

Note

To unlock your admin account or any sysadmin account locked due to expiry or invalid attempts, refer to [Unlock or Recover a User Account for Sysadmin or Any Admin User](#)

Set User Permissions

Perform the following procedure to set permissions for a normal user to execute privilege commands:

1. To add permission on a particular command, enter the following command:

```
# chmod +s <absolute_path_to_command_binary_file>
```

For example, to add the setuid permission on `passwd` command, enter the following

```
# chmod +s /usr/bin/passwd
```

2. To remove permission on a particular command, enter the following command as:

```
# chmod -s <absolute_path_to_command_binary_file>
```

For example, to remove the setuid permission on passwd command, enter the following command:

```
# chmod -s /usr/bin/passwd
```

Modify Passwords

You can change the password, modify its aging, and perform several other tasks. See the following topics for information:

Modifying Password Aging

Perform the following procedure to modify the password aging:

1. Log on as insight user.
2. Change to root user.
3. Modify `maximum password aging days` field:

```
chage -M <MAX_PASS_DAYS> <username>
```

By default, the password expires in 90 days.

For example: If the username is user01 and maximum password aging days is 90, then enter the following:

```
chage -M 90 user01
```

Restricting the User to Change Password on First Login

Perform the following procedure to create first password and force the user to change password on first login:

1. Log on as insight user.
2. Change to root user.
3. After creating the user, assign a default password:

```
# passwd <username>
```

For example, if the username is user01, then enter the following:

```
passwd user01
```

4. Compel the user to change the password during first time login:

```
chage -d 0 <username>
```

For example, if the username is user01, then enter the following:


```
chage -d 0 user01
```

Change Password

Perform the following procedure if root user needs to change the other user password:

1. To change the other user password as a root user, enter the following command:

```
passwd <username>
```

For example, if the username is user01, then enter the following:

```
passwd user01
```

2. To change your own password, enter the following command:

```
passwd
```

Modify User Session Timeout Interval

Perform the following procedure to modify the user session timeout interval.

1. Log on as insight user.
2. Change to root user.
3. Modify `ClientAliveInterval` property:

```
# vi /etc/ssh/sshd_config
```

The `ClientAliveInterval` is calculated in seconds. By default, the user session time-out interval is 750 seconds.

For example, if session time-out interval is one hour, then enter 3600 seconds.

```
ClientAliveInterval 3600
```

4. Restart sshd server using "service sshd restart":

```
# service sshd restart
```

Limit the Maximum Number of Login Sessions

For each Ribbon Application Management Platform (RAMP) user, the maximum number of login sessions in a system are currently limited, by default, to 10. The maximum limit is configurable for all users except a root user.

Perform the following procedure to limit the maximum login sessions for each user:

- Execute the following command as `root` user:

```
cat /etc/security/limits.conf
```

Where, `#<domain>`, `<type>`, `<item>` and `<value>` are used for informational purpose and do not appear in the actual output.

Additionally, you can modify the login limit for a particular user or group.

Modifying the login limit for a user

If a particular user has specific login limits, the following entry can be used where the `<username>` must be replaced with actual user name and value can be modified as per requirement:

```
# <domain>      <type>      <item>      <value>
@<username>    hard          5
```

Modifying the login limit for a group

If a particular group has specific login limits, then the following entry can be used where `<groupname>` must be replaced with actual group name and value can be modified as per requirement:

```
# <domain>      <type>      <item>      <value>
@<groupname>    hard          4
```

Configure User Account Lock Settings

If a user of the Ribbon Application Management Platform (RAMP) enters an incorrect password for more than the configured limit (default: 5), the user's account is locked for the configured time (default: 10 minutes). During this time period, the user cannot log on even with the correct password.

Use this procedure to specify settings for locking user accounts:

Start

1. Log in as `admin` user.
2. Change to `root` user:

```
sudo su -
```

3. Navigate to `/etc/security/` and edit the `faillock.conf` file:

```
/etc/security/faillock.conf
```

Uncomment the pre-defined settings in the `faillock.conf` file to edit the values:

- a. `fail_interval = 900`
- b. `silent`
- c. `audit`
- d. `unlock_time = 900`

- e. `dir = /var/log/faillock`
- f. `deny = 5`
- g. `even_deny_root`
- 4. Edit the `unlock_time` value to specify the time, in seconds, before unlocking a user's password.
- 5. Edit the `deny` value to specify the number of failed password attempts before locking a user account.

Enable Users to Create Cron Jobs

Use the following procedure to enable users to create cron jobs.

1. Ensure that the user does not exist in the `/etc/cron.deny` file.
2. Add the user to the `/etc/cron.allow` file.

Enable Users to Create 'at' Jobs

Use the following procedure to enable users to create `at` jobs.

1. Ensure that the user does not exist in the `/etc/at.deny` file.
2. Add the user to the `/etc/at.allow` file.

Establish Passwordless Connection from an External Server to RAMP

Use this procedure to establish the passwordless connection from an external server (remote server) to the Ribbon Application Management Platform (RAMP) device.

Start

1. Log on to the remote server.
2. Copy the RAMP user private key to the remote server.
For example, you can copy the file `cloud_ats_ems.key` to the `/tmp` directory in the remote server `fd00:10:6b50:5c30::1c`.
To generate the SSH keys, refer to [Generate SSH Keys for RAMP Users](#).
3. Create a file `~/.ssh/config` and add the following content:

```
Host <IP Address of RAMP Server>
  Port 22
  User <UserName>
  IdentityFile <absolute path of the RAMP private key file>
```

Example:

```
Host fd00:10:6b50:5c30::1c
  Port 22
  User admin
  IdentityFile /tmp/cloud_ats_ems.key
```

4. Enter the following command:

```
ssh-copy-id -f -i <public key file of the remote server> <the RAMP user>@<RAMP IP>
```

Example:

```
/usr/bin/ssh-copy-id -f -i ~/.ssh/id_rsa.pub admin@fd00:10:6b50:5c30::1c
```

Sample output:

```
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/
id_rsa.pub"
#####
#
# This system is restricted to authorized users only.      #
# Unauthorized access or access attempts to this system  #
# or services are prohibited. All user activity is logged. #
# Evidence of unauthorized use collected during monitoring #
# may be provided to appropriate personnel for           #
# administrative, criminal or other adverse action.      #
#
#####

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'admin@fd00:10:6b50:5c30::1c'"
and check to make sure that only the key(s) you wanted were added.
```

5. Test the passwordless communication by entering the following command on the remote server:

```
ssh <the RAMP user>@<the RAMP IP address>
```

Example:

```
ssh admin@fd00:10:6b50:5c30::1c
```

Establish RAMP CNF Active-Standby Instance Passwordless Connection

Passwordless SSH Connection

Perform the following procedure to ensure a passwordless SSH connection between the RAMP active and standby instances and vice-versa.

1. Log onto the RAMP active instance as the `admin` user.
2. Change to insight user:

```
su - insight
```

3. Navigate to the `.ssh` directory:

```
cd .ssh
```

4. SSH to the RAMP standby instance:

```
ssh insight@<IP address of the RAMP standby instance>
```

If the SSH password-less connection is intact, you are not prompted for a password.

5. Log on to the RAMP standby instance as the `admin` user.
6. Change to insight user: :

```
su - insight
```

7. Navigate to the `.ssh` directory:

```
cd .ssh
```

8. SSH to the RAMP standby instance:

```
ssh insight@<IP address of the RAMP active instance>
```

If the SSH password-less connection is intact, you are not prompted for a password.

Change the GRUB Password

Ribbon recommends changing all default passwords as a security best practice.

The Grub password protects the boot loader.

Start:

1. Access RAMP as the admin user.
2. Change to the root user:

```
sudo su -
```

3. Enter the command:

```
grub2-setpassword
```

The following message displays:

```
Enter password:
```

4. Enter the password. The following message displays:

```
Confirm password:
```

5. Enter the password again.

Managing Log Files

In this section:

- [Change Log Level](#)
- [Configure Silent Auth for Jboss CLI](#)
- [RAMP Log Files](#)
- [Reset Admin Password for Jboss CLI](#)

The Ribbon Application Management Platform (RAMP) lists the available log files, allows you to change the log file locations, and levels.

Change Log Level

In this section

- [Change the Log Level to DEBUG](#)
- [Change the Log Level to INFO](#)

The Ribbon Application Management Platform (RAMP) allows you to change the log level. You need not restart JBoss for the changes to take effect.

Note

`Silent Auth` is enabled (on) in RAMP by default.

To run the JBoss CLI command:

The username is: admin

The default password is: Sonus@123

If you forget the admin JBoss CLI password or need to reset, refer to [Reset Admin Password for Jboss CLI](#).

Prerequisite

RAMP is and running.

Change the Log Level to DEBUG

Use this procedure to change the log level to DEBUG:

Start

1. Log on to the RAMP as `Insight` user. For more information, refer to [Log onto the RAMP CLI](#).
2. Navigate to the following directory:

```
cd /opt/sonus/jboss/bin
```

3. Run the following command to list the current settings of all loggers:
Do not use username and password when `Silent Auth` is enabled. To check the status of `Silent Auth` for JBoss CLI, refer to [Configure Silent Auth for Jboss CLI](#).

```
./jboss-cli.sh --user=admin --password=Sonus@123 -c "/subsystem=logging/  
logger=*:read-resource" | egrep 'logger|level'
```

Example output

```
./jboss-cli.sh --user=admin --password=Sonus@123 -c "/subsystem=logging/  
logger=*:read-resource" | egrep 'logger|level'  
    ("logger" => "com.sonus.agent.framework")  
    "level" => "INFO",  
    ("logger" => "com.sonus.ems.unity")  
    "level" => "INFO",  
    ("logger" => "org.apache.sshd")  
    "level" => "ERROR",  
    ("logger" => "com.sonus.ems.push.server")  
    "level" => "INFO",  
    ("logger" => "com.sonus.ems.session")  
    "level" => "INFO",
```

```
("logger" => "com.sonus.vnf.vim.openstack.auditor")
"level" => "DEBUG",
("logger" => "com.sonus.ems.security")
"level" => "INFO",
("logger" => "com.sonus.report")
"level" => "INFO",
("logger" => "com.sonus.ems.nhr")
"level" => "INFO",
("logger" => "com.sonus.ems.ual")
"level" => "INFO",
("logger" => "com.sonus.deviceInventory")
"level" => "INFO",
("logger" => "com.sonus.ems.gsxUpgrade")
"level" => "INFO",
("logger" => "com.sonus.ems.lnp")
"level" => "INFO",
("logger" => "com.sonus.ems.fm.trapResync")
"level" => "INFO",
("logger" => "com.sonus.ems.mnp")
"level" => "INFO",
("logger" => "mnp.audit.telcordia")
"level" => "INFO",
("logger" => "mnp.audit.syniverse")
"level" => "INFO",
("logger" => "mnp.audit.genericNP")
"level" => "INFO",
("logger" => "org.quartz")
"level" => "INFO",
("logger" => "TR746")
"level" => "INFO",
("logger" => "TR746-BYTES")
"level" => "INFO",
("logger" => "com.sonus.ems.hornet")
"level" => "INFO",
("logger" => "com.sonus.ems.cluster.partialConfigUpdate")
"level" => "INFO",
("logger" => "CLICmds")
"level" => "INFO",
("logger" => "com.sonus.ems.sbx.cli")
"level" => "INFO",
("logger" => "CliFramework")
"level" => "INFO",
("logger" => "com.sonus.RmtProcessProxy")
"level" => "INFO",
("logger" => "com.sonus.ems.licmgmt")
"level" => "INFO",
("logger" => "com.sonus.EntityMgr")
"level" => "INFO",
("logger" => "com.sonus.Listall")
"level" => "INFO",
("logger" => "com.sonus.SmsApi")
"level" => "INFO",
("logger" => "com.sonus.SmsApi.SOAP")
```



```
"level" => "INFO",
("logger" => "com.sonus.ems.api")
"level" => "INFO",
("logger" => "com.sonus.ems.api.SOAP")
"level" => "INFO",
("logger" => "com.sonus.ems.vlan.web")
"level" => "INFO",
("logger" => "com.sonus.ems.vlan.core")
"level" => "INFO",
("logger" => "com.sonus.sbcapi.SOAP")
"level" => "INFO",
("logger" => "com.sonus.ems.api.prov")
"level" => "INFO",
("logger" => "emsapi.security.log")
"level" => "INFO",
("logger" => "com.rbbn.pm.metadata")
"level" => "INFO",
("logger" => "com.sonus.ems.apacheproxy")
"level" => "INFO",
("logger" => "com.sonus.ems.fm")
"level" => "INFO",
("logger" => "com.sonus.ems.fm.audit.FMSystemAuditor")
"level" => "INFO",
("logger" => "com.sonus.ems.uiGen")
"level" => "INFO",
("logger" => "com.sonus.ems.tm")
"level" => "INFO",
("logger" => "org.hibernate")
"level" => "INFO",
("logger" => "com.sonus.ssh")
"level" => "INFO",
("logger" => "SshAuditLog")
"level" => "INFO",
("logger" => "com.sonus.ems.sgx.adax")
"level" => "INFO",
("logger" => "audit.com.sonus.ems.reachability")
"level" => "INFO",
("logger" => "com.sonus.ems.lawfulintercept")
"level" => "INFO",
("logger" => "com.sonus.ems.hornet.MetadataDump")
"level" => "INFO",
("logger" => "com.sonus.ems.sgxapi")
"level" => "INFO",
("logger" => "com.sonus.ems.security.EmsAuthLogs")
"level" => "INFO",
("logger" => "com.sonus.UserActivityLog")
"level" => "INFO",
("logger" => "com.sonus")
"level" => "INFO",
("logger" => "org.apache.axis")
"level" => "INFO",
("logger" => "com.sonus.ems.dashboard")
"level" => "INFO",
```

```

(logger" => "com.sonus.ems.ndgui")
"level" => "INFO",
(logger" => "com.sonus.ems.ndgui.node.NodeDetailsHelper")
"level" => "INFO",
(logger" => "org.apache.myfaces")
"level" => "INFO",
(logger" => "org.apache.kafka")
"level" => "INFO",
(logger" => "Owasp.CsrfGuard")
"level" => "INFO",
(logger" => "org.jboss.as.ejb3.deployment.processors")
"level" => "INFO",
(logger" => "org.jboss.resteasy.plugins.server.servlet")
"level" => "INFO",
(logger" => "org.jboss.as.ee")
"level" => "INFO",
(logger" => "org.jboss.as.dependency")
"level" => "INFO",
(logger" => "org.jboss.as.messaging")
"level" => "INFO",
(logger" => "org.jboss.as.server.deployment.scanner")
"level" => "INFO",
(logger" => "org.jboss.as.jpa")
"level" => "INFO",
(logger" => "org.jboss.resteasy.spi.ResteasyDeployment")
"level" => "INFO",
(logger" => "org.jboss.ws.cxf.metadata")
"level" => "INFO",
(logger" => "org.hornetq.core.server")
"level" => "INFO",
(logger" => "net.sf.ehcache")
"level" => "INFO",
-bash-4.2$

```

4. Run the following command:

```

./jboss-cli.sh --user=admin --password=Sonus@123 -c "/subsystem=logging/
logger=<Name of the logger category>:add"

```

Refer to Logger List.

Example output

```

./jboss-cli.sh --user=admin --password=Sonus@123 -c "/subsystem=logging/
logger=com.sonus.logging.category:add"

```

If the operation is successful, the following is displayed.

Output

```
{"outcome" => "success"}
```

- To change the log level to DEBUG, type the following (replace `com.sonus.logging.category` with the correct logger name), and run:

```
./jboss-cli.sh --user=admin --password=Sonus@123 -c "/subsystem=logging/  
logger=com.sonus.logging.category:write-attribute(name=level,value=DEBUG)"
```

If the operation is successful, the following output is displayed.

```
{"outcome" => "success"}
```

Note

Once the issue is reproduced, you must set the loggers to INFO for the loggers that you set the level to DEBUG.

Change the Log Level to INFO

Use the following procedure to change the log level to INFO:

Start

- Log on to the RAMP as the `Insight` user.
- Navigate to the following directory:

```
cd /opt/sonus/jboss/bin
```

- Run the following command:

```
./jboss-cli.sh --user=admin --password=Sonus@123 -c "/subsystem=logging/  
logger=<Name of the logger category>:write-attribute(name=level,value=INFO)"
```

See Logger List. The following is displayed:

Example output

```
./jboss-cli.sh --user=admin --password=Sonus@123 -c "/subsystem=logging/  
logger=com.sonus.logging.category:write-attribute(name=level,value=INFO)"
```

If the operation is successful, the following is displayed.

Output

```
{"outcome" => "success"}
```

4. Remove the logging category created in Step 3, and run the following command:

```
./jboss-cli.sh --user=admin --password=Sonus@123 -c "/subsystem=logging/  
logger=<Name of the logger category>:remove"
```

Example output

```
./jboss-cli.sh --user=admin --password=Sonus@123 -c "/subsystem=logging/  
logger=com.sonus.logging.category:remove"
```

If the operation is successful, the following is displayed.

Output

```
{"outcome" => "success"}
```

The following table represents the logger list:

Logger Name	Log Level
audit.com.sonus.ems.reachability	INFO
audit.com.sonus.ems.reachability.server.ReachabilityMgr	INFO
class com.sonus.ems.pm.server.helpers.ConfigDataHelper	INFO
com.sonus	INFO
com.sonus.AcAdminServlet	INFO
com.sonus.access	INFO
com.sonus.access.dao.ProtectionGroupAssociationDAO	INFO
com.sonus.access.drManagement.DrNodeNotificationReceiver	INFO
com.sonus.access.events.EventTopicSubscriber	INFO

Logger Name	Log Level
com.sonus.access.events.NotificationHelper	INFO
com.sonus.access.mbean.DrAutomationService	INFO
com.sonus.AcctSyncMgr	INFO
com.sonus.ADAXAgtMgr	INFO
com.sonus.agent.framework	WARN
com.sonus.agent.framework.instr.procMgmt.SimplePortListener	WARN
com.sonus.agent.framework.instr.procMgmt.SimplePortResponder	WARN
com.sonus.AgentAdmin	INFO
com.sonus.AgentDiscov	INFO
com.sonus.BaseDB	INFO
com.sonus.callAnalysis.CallAnalysisPurgerMgr	INFO
com.sonus.callAnalysis.CallAnalysisPurgerService	INFO
com.sonus.callAnalysis.NotificationHelper	INFO
com.sonus.callAnalysis.scheduler.SchedulingUtil	INFO
com.sonus.CLI	INFO
com.sonus.common.dao.ac.AccessControlDAO	INFO
com.sonus.common.dao.ac.PartitionDAO	INFO
com.sonus.common.dao.ac.RoleDAO	INFO
com.sonus.common.dao.ac.UserDAO	INFO
com.sonus.common.dao.ac.UserPasswordDAO	INFO
com.sonus.common.dao.BaseDAO	INFO

Logger Name	Log Level
com.sonus.common.dao.cluster.ClusterDAO	INFO
com.sonus.common.dao.EncryptedBlobUserType	INFO
com.sonus.common.dao.EncryptedEncodedStringUserType	INFO
com.sonus.common.dao.EncryptedStringUserType	INFO
com.sonus.common.dao.HibernateDBUtil	INFO
com.sonus.common.dao.node.NodeDAO	INFO
com.sonus.common.dao.StoredProcSequenceGenerator	INFO
com.sonus.common.naming.ContextFactory	INFO
com.sonus.common.naming.ContextHelper	INFO
com.sonus.common.txmgt.TransactionManagement	INFO
com.sonus.DBConnPool	INFO
com.sonus.DBConnPoolX	INFO
com.sonus.DevGroupMgr	INFO
com.sonus.deviceInventory	INFO
com.sonus.deviceInventory.discover.DeviceInventoryMgr	INFO
com.sonus.deviceInventory.mbean.DeviceInventoryService	INFO
com.sonus.deviceInventory.notification.NotificationHelper	INFO
com.sonus.deviceInventory.scheduler.SchedulingUtil	INFO
com.sonus.DiscoveryDB	INFO
com.sonus.DSIagtMgr	INFO
com.sonus.DSSIM	INFO

Logger Name	Log Level
com.sonus.ems.ac.server.acmgr.AccessControlMgr	INFO
com.sonus.ems.ac.server.helpers.RoleUtils	INFO
com.sonus.ems.ac.server.proxy.AppService	INFO
com.sonus.ems.ac.server.resourcegroupmgr.ResourceGroupMgr	INFO
com.sonus.ems.ac.server.rolemgr.RoleMgr	INFO
com.sonus.ems.ac.server.usermgr.UserMgr	INFO
com.sonus.ems.ac.ui.ResourceGroupServlet	INFO
com.sonus.ems.ac.utils.ResourceGroupUtils	INFO
com.sonus.ems.ac.utils.ServerProxy	INFO
com.sonus.ems.apacheproxy	INFO
com.sonus.ems.apacheproxy.ApacheProxyNodeMgr	INFO
com.sonus.ems.apacheproxy.SBX5KNodeApacheProxyUtil	INFO
com.sonus.ems.api	INFO
com.sonus.ems.api.deployer	DEBUG
com.sonus.ems.api.deployer.APIDeployer	DEBUG
com.sonus.ems.api.prov	INFO
com.sonus.ems.api.psx.r09_02_00.mapping.PSXMapper	INFO
com.sonus.ems.api.SOAP	INFO
com.sonus.ems.cluster.mgr.ClusterCMgmtInitializer	INFO
com.sonus.ems.cluster.mgr.ClusterJobManager	INFO
com.sonus.ems.cluster.mgr.ClusterMgr	INFO

Logger Name	Log Level
com.sonus.ems.cluster.purger.ClusteredNodePurger	INFO
com.sonus.ems.cluster.update.ClusteredNodeStatusChange	INFO
com.sonus.ems.cluster.web.ClusterSchedulerInitServlet	INFO
com.sonus.ems.clusterapi.rest.api.ClusterNodeStatus	INFO
com.sonus.ems.clusterapi.rest.api.Configuration	INFO
com.sonus.ems.clusterapi.rest.api.DryUpNode	INFO
com.sonus.ems.clusterapi.rest.api.DryUpVNFNode	INFO
com.sonus.ems.clusterapi.rest.api.exception.ClusterMgmtExceptionHandler	INFO
com.sonus.ems.clusterapi.rest.api.RegisterNode	INFO
com.sonus.ems.clusterapi.rest.api.RetrieveClusters	INFO
com.sonus.ems.clusterapi.rest.api.RetrievePMDData	INFO
com.sonus.ems.clusterapi.rest.api.VNF2VNFMapping	INFO
com.sonus.ems.clusterapi.rest.security.ResponseInterceptor	INFO
com.sonus.ems.clusterapi.rest.security.SecurityInterceptor	INFO
com.sonus.ems.clusterapi.rest.util.ClusterMgmtUtils	INFO
com.sonus.ems.CmfAuthorizationFilter	INFO
com.sonus.ems.common	DEBUG
com.sonus.ems.common.NodeChangeSubscriber	DEBUG
com.sonus.ems.common.NodeChangeSubscriberImpl	DEBUG
com.sonus.ems.common.SystemMgrInit	DEBUG
com.sonus.ems.config.CpuPropertyEvaluator	INFO

Logger Name	Log Level
com.sonus.ems.config.PersisterService	INFO
com.sonus.ems.config.PropertiesService	INFO
com.sonus.ems.config.XMLConfigService	INFO
com.sonus.ems.dashboard	INFO
com.sonus.ems.database.EmsBaseDBLibrary	INFO
com.sonus.ems.database.EmsDBConnectionPool	INFO
com.sonus.ems.database.EmsDBConnectionPool1	INFO
com.sonus.ems.database.Utills	INFO
com.sonus.ems.event.AsyncChangePublisher	INFO
com.sonus.ems.event.ChangePublisher	INFO
com.sonus.ems.fm	INFO
com.sonus.ems.fm.audit.FMSystemAuditor	INFO
com.sonus.ems.fm.db.api.FMServerAPI	INFO
com.sonus.ems.fm.db.FMServiceLocator	INFO
com.sonus.ems.fm.db.OmniBusDAOFactory	INFO
com.sonus.ems.fm.db.OmniBusEventDAO	INFO
com.sonus.ems.fm.db.OmniBusFMUserDAO	INFO
com.sonus.ems.fm.eventset.api.FMModelChangeMessenger	INFO
com.sonus.ems.fm.eventset.EventSetDirector	INFO
com.sonus.ems.fm.eventset.FMModelChangePublisher	INFO
com.sonus.ems.fm.historical.DbPersister	INFO

Logger Name	Log Level
com.sonus.ems.fm.historical.EventArchiver	INFO
com.sonus.ems.fm.mbean.EventArchiverService	INFO
com.sonus.ems.fm.mbean.FMService	INFO
com.sonus.ems.fm.trap	DEBUG
com.sonus.ems.fm.trapResync	INFO
com.sonus.ems.fm.ui.init.FMInitServlet	INFO
com.sonus.ems.fm.ui.proxy.FMEventPurgerTask	INFO
com.sonus.ems.fm.ui.proxy.InsightServiceProxy	INFO
com.sonus.ems.fm.ui.view.ActiveViewDirector	INFO
com.sonus.ems.fm.ui.view.nodes.SourceAddressNodeListerner	INFO
com.sonus.ems.fm.ui.view.TFProfileAdminCtlServlet	INFO
com.sonus.ems.fm.ui.web.FMEventListServlet	INFO
com.sonus.ems.fm.ui.web.FMUpdater	INFO
com.sonus.ems.fm.ui.web.FMUpdaterModelChangeSubscriber	INFO
com.sonus.ems.gsxsystem.CommandsHandler	INFO
com.sonus.ems.gsxUpgrade	INFO
com.sonus.ems.gsxUpgrade.auditLog.AuditLogPurgerTask	INFO
com.sonus.ems.gsxUpgrade.dao.UpgradeJobDAO	INFO
com.sonus.ems.gsxUpgrade.dao.UpgradeTaskDAO	INFO
com.sonus.ems.gsxUpgrade.mbean.GsxUpgradeConfigListener	INFO
com.sonus.ems.gsxUpgrade.mbean.GsxUpgradeService	INFO

Logger Name	Log Level
com.sonus.ems.gsxUpgrade.operations.UpgradeJobMgr	INFO
com.sonus.ems.GsxUpgradeAuthorizationFilter	INFO
com.sonus.ems.ha.HAStateTransition	INFO
com.sonus.ems.hornet	INFO
com.sonus.ems.hornet.common.CommonUtils	INFO
com.sonus.ems.hornet.mbean.HornetMgmtConfigListener	INFO
com.sonus.ems.hornet.mbean.HornetMgmtService	INFO
com.sonus.ems.hornet.MetadataDump	INFO
com.sonus.ems.hornet.MetadataDumpSvt	INFO
com.sonus.ems.hornet.model.loader.ConfSpecLoader	INFO
com.sonus.ems.hornet.model.loader.ModelOverlayLoader	INFO
com.sonus.ems.hornet.model.loader.SBX5KConfSpecLoader	INFO
com.sonus.ems.hornet.model.metadata.DefinedType	INFO
com.sonus.ems.hornet.model.metadata.EnumVal	INFO
com.sonus.ems.hornet.model.metadata.EnumValType	INFO
com.sonus.ems.hornet.model.metadata.Key	INFO
com.sonus.ems.hornet.model.metadata.KeyRef	INFO
com.sonus.ems.hornet.model.metadata.MetadataAttribute	INFO
com.sonus.ems.hornet.model.metadata.MetadataManagedObject	INFO
com.sonus.ems.hornet.model.metadata.MetadataMgr	INFO
com.sonus.ems.hornet.model.metadata.ModelRepository	INFO

Logger Name	Log Level
com.sonus.ems.hornet.model.metadata.Operation	INFO
com.sonus.ems.hornet.model.metadata.Range	INFO
com.sonus.ems.hornet.model.metadata.UIFieldOverlays	INFO
com.sonus.ems.hornet.workflow.WorkFlowManager	INFO
com.sonus.ems.init.InsightIsInitializedServlet	INFO
com.sonus.ems.lawfulintercept	INFO
com.sonus.ems.layoutmgr.LayoutmgrService	INFO
com.sonus.ems.layoutmgr.ServerProxy	INFO
com.sonus.ems.lnp	INFO
com.sonus.ems.mnp	INFO
com.sonus.ems.mnp.core.AbstractMNPServiceManager	INFO
com.sonus.ems.mnp.core.dao.MnpBddDAO	INFO
com.sonus.ems.mnp.core.HostedLnpProvisioner	INFO
com.sonus.ems.mnp.core.MNPServiceManagerFactory	INFO
com.sonus.ems.mnp.core.MnpUtils	INFO
com.sonus.ems.mnp.syniverse.impl.MnpServiceImpl	INFO
com.sonus.ems.mnp.syniverse.impl.SyniverseMNPServiceManager	INFO
com.sonus.ems.mnp.telcordia.impl.NPCWebServiceImpl	INFO
com.sonus.ems.ndgui	INFO
com.sonus.ems.ndgui.alarms.AlarmUpdateHandler	INFO
com.sonus.ems.ndgui.jsf.CustomServletContextListener	INFO

Logger Name	Log Level
com.sonus.ems.ndgui.jsf.NDGuiSessionListener	INFO
com.sonus.ems.ndgui.node.NodeDetailsHelper	INFO
com.sonus.ems.ndgui.webapp.NDGUISessionThreadMonitor	INFO
com.sonus.ems.nhr	INFO
com.sonus.ems.nhr.DBApi	INFO
com.sonus.ems.nhr.Init	INFO
com.sonus.ems.nhr.NotificationHelper	INFO
com.sonus.ems.nhr.PurgerTask	INFO
com.sonus.ems.nhr.ReportMgr	INFO
com.sonus.ems.nodeadmin.mgr.NodeAdminCMgmtInitializer	INFO
com.sonus.ems.nodeadmin.mgr.NodeAdminJobManager	INFO
com.sonus.ems.nodeadmin.mgr.NodeMgr	INFO
com.sonus.ems.nodeadmin.ui.NodeAdminSchedulerInitServlet	INFO
com.sonus.ems.persistence.MigrationInfoXMLReader	INFO
com.sonus.ems.persistence.ObjectPersister	INFO
com.sonus.ems.persistence.PropertiesHandler	INFO
com.sonus.ems.persistence.TableMgr	INFO
com.sonus.ems.push.server	INFO
com.sonus.ems.radius.mbean.RadiusCfg	INFO
com.sonus.ems.radius.mbean.RadiusConfigListener	INFO
com.sonus.ems.radius.mbean.RadiusService	INFO

Logger Name	Log Level
com.sonus.ems.radius.mbean.RadiusSystemConfigListener	INFO
com.sonus.ems.radius.mbean.RadiusSystemService	INFO
com.sonus.ems.reachability	ERROR
com.sonus.ems.reportframework.DeviceReportMgr	INFO
com.sonus.ems.reportframework.IndexHelper	INFO
com.sonus.ems.reportframework.ReportManager	INFO
com.sonus.ems.reportframework.ReportManager-verbose	INFO
com.sonus.ems.reports.user.PurgerTask	INFO
com.sonus.ems.sbc.framework.collector.InventoryCollector	INFO
com.sonus.ems.sbc.framework.mgr.SBCJobManager	INFO
com.sonus.ems.sbc.framework.mgr.SBCMgmtInitializer	INFO
com.sonus.ems.sbc.framework.monitor.SBCJobStatusMonitor	INFO
com.sonus.ems.sbc.framework.monitor.SBCPartialTaskMonitor	INFO
com.sonus.ems.sbc.framework.utils.ConfigVersionUtil	INFO
com.sonus.ems.sbc.framework.utils.SBCJobUtils	INFO
com.sonus.ems.sbc.framework.utils.SBCNodeCache	INFO
com.sonus.ems.sbc.framework.utils.SBCUserResourceGroupCache	INFO
com.sonus.ems.sbc.framework.web.SBCSchedulerInitServlet	INFO
com.sonus.ems.sbc.NotificationHelper	INFO
com.sonus.ems.sbx.cli	INFO
com.sonus.ems.sbx5k.localWeb.SessionFilter	INFO

Logger Name	Log Level
com.sonus.ems.security	INFO
com.sonus.ems.security.EmsAuthLogs	INFO
com.sonus.ems.security.JBossLoginModule	INFO
com.sonus.ems.security.UserActivityFilter	INFO
com.sonus.ems.session	INFO
com.sonus.ems.session.Session	INFO
com.sonus.ems.sgx.adax	INFO
com.sonus.ems.sgx4000.license.Sgx4000LicensableImpl	INFO
com.sonus.ems.sgxapi	INFO
com.sonus.ems.tgwizard.FinishTgPanel	INFO
com.sonus.ems.tgwizard.GsxHelper	INFO
com.sonus.ems.tgwizard.IsupProfilePanel	INFO
com.sonus.ems.tgwizard.ModelHelper	INFO
com.sonus.ems.tgwizard.MrtHelper	INFO
com.sonus.ems.tgwizard.PsxHelper	INFO
com.sonus.ems.tgwizard.StartTgPanel	INFO
com.sonus.ems.tgwizard.TgCicsPanel	INFO
com.sonus.ems.tgwizard.TgProfilePanel	INFO
com.sonus.ems.tgwizard.TgPsxInfoPanel	INFO
com.sonus.ems.tgwizard.TgResourcesPanel	INFO
com.sonus.ems.tgwizard.TgWizardMgr	INFO

Logger Name	Log Level
com.sonus.ems.tgwizard.WizardPanel	INFO
com.sonus.ems.threadpool.ThreadPool-IncreaseThreadPoolSize	INFO
com.sonus.ems.threadpool.ThreadPool-Watchdog	INFO
com.sonus.ems.ual	INFO
com.sonus.ems.ual.Init	INFO
com.sonus.ems.ual.NotificationHelper	INFO
com.sonus.ems.ual.UserActivityAuditLogDatabaseHelper	INFO
com.sonus.ems.ual.UserActivityAuditLogGeneratorTask	INFO
com.sonus.ems.ual.UserActivityAuditLogPurgeTask	INFO
com.sonus.ems.uiGen	INFO
com.sonus.ems.unity	INFO
com.sonus.ems.unity.expCore.localWeb.CacheFilter	INFO
com.sonus.ems.unity.expCore.localWeb.SessionFilter	INFO
com.sonus.ems.unity.expCore.mbean.CoreMgmtLocalService	INFO
com.sonus.ems.unity.expCore.webSvc.auth.WebSvcSecurityInterc eptor	INFO
com.sonus.ems.unity.mgmt.auth.WebSvcSecurityInterceptor	INFO
com.sonus.ems.unity.mgmtMeta.auth.WebSvcSecurityInterceptor	INFO
com.sonus.ems.vlan.core	INFO
com.sonus.ems.vlan.web	INFO
com.sonus.EntityMgr	INFO
com.sonus.FiMigration	INFO

Logger Name	Log Level
com.sonus.FMAudioAlm	INFO
com.sonus.General	INFO
com.sonus.Gsx9000Svc	INFO
com.sonus.InventoryDB	INFO
com.sonus.JdmkConnMgr	INFO
com.sonus.JmxEvtMgr	INFO
com.sonus.Listall	INFO
com.sonus.LockMgr	INFO
com.sonus.LogMgr	INFO
com.sonus.ME9000Svc	INFO
com.sonus.NeapRMIMgr	INFO
com.sonus.NESvcs	INFO
com.sonus.NodeMgr	INFO
com.sonus.ObjectNav	INFO
com.sonus.PifCollect	INFO
com.sonus.PifCollectX	INFO
com.sonus.PifRead	INFO
com.sonus.PifReadX	INFO
com.sonus.PifSchedule	INFO
com.sonus.PMClient	INFO
com.sonus.PMDataCol	INFO

Logger Name	Log Level
com.sonus.ProxyMgr	INFO
com.sonus.PSXConnMgmt	INFO
com.sonus.PsxConnMgr	INFO
com.sonus.PushMsg	INFO
com.sonus.Reachability	INFO
com.sonus.RmtProcessProxy	INFO
com.sonus.RmtRuntime	INFO
com.sonus.RoleMgr	INFO
com.sonus.RpAdminMgr	INFO
com.sonus.RprtFrmwrk	INFO
com.sonus.SASAgMgr	INFO
com.sonus.SBAPI	INFO
com.sonus.sbcapi.SOAP	INFO
com.sonus.Scheduler	INFO
com.sonus.SecurityMgr	INFO
com.sonus.SessionMgr	INFO
com.sonus.SockPoolMgr	INFO
com.sonus.SRXAgMgr	INFO
com.sonus.ssh	INFO
com.sonus.SSHMgr	INFO
com.sonus.SvcCtrlMgr	INFO

Logger Name	Log Level
com.sonus.SysMgr	INFO
com.sonus.TaskBldr	INFO
com.sonus.TelnetMgr	INFO
com.sonus.TFProfMgr	INFO
com.sonus.TgProv	INFO
com.sonus.TGroupDB	INFO
com.sonus.TgWizard	INFO
com.sonus.ThreadPool	INFO
com.sonus.TL1AgtMgr	INFO
com.sonus.TmsDisc	INFO
com.sonus.TmsGui	INFO
com.sonus.TmsProv	INFO
com.sonus.TmsRule	INFO
com.sonus.TmsSys	INFO
com.sonus.TmsThreshld	INFO
com.sonus.UserActivDB	INFO
com.sonus.UserMgr	INFO
com.sonus.vnf.vim.openstack.auditor	DEBUG
com.sonus.WBEM	INFO
emsapi.security.log	INFO
mnnp.audit.genericNP	INFO

Logger Name	Log Level
mnmp.audit.syniverse	INFO
mnmp.audit.telcordia	INFO
org.apache.axis	INFO
org.apache.myfaces	INFO
org.hibernate	INFO
org.quartz	INFO
SshAuditLog	INFO

Configure Silent Auth for Jboss CLI

The Ribbon Application Management Platform (RAMP) allows you to enable or disable Silent Auth for JBoss CLI.

Note

- Silent Auth is enabled on the RAMP by default.
- Silent Auth on: User password is not needed for running JBoss CLI commands.
- Silent Auth off: User password is needed for running JBoss CLI commands.
- Do not use username and password when Silent Auth is enabled.
- To check if Silent Auth is enabled, use: `./configureJbossCliSilentAuth.sh status`

Prerequisite

RAMP is up and running.

Start

Use this procedure to enable or disable Silent Auth.

1. Log on to the RAMP as an Insight user. For more information, refer to [Log onto the RAMP CLI](#).
2. Navigate to `/opt/sonus/ems/conf/security/` and to know the working of this script usage:

Example

```
-bash-4.4$ ./configureJbossCliSilentAuth.sh -help
```

Example output

```
Usage: ./configureJbossCliSilentAuth.sh on/off jboss_cli_password
```

```
Usage: ./configureJbossCliSilentAuth.sh status
```

```
    on:      Enable Silent Auth for Jboss Cli
```

```
    off:     Disable Silent Auth for Jboss Cli
```

```
    status:  Check Silent Auth for Jboss Cli, Enabled means no user name/
paswrk asked for running jboss cli cmds.
```

```
           Disabled means user name/paswrk asked for running jboss cli cmds
```

Note

If you forgot the admin JBoss CLI password or need to reset, refer to [Reset Admin Password for Jboss CLI](#).

3. Check the current state of `Silent Auth`:

```
./configureJbossCliSilentAuth.sh status
```

Example output

```
Silent Auth is enabled
```

4. If you want to disable `Silent Auth`:

```
-bash-4.4$ ./configureJbossCliSilentAuth.sh off <jboss_cli_password>
```

Example output

```
Disabling Silent Auth for Jboss Cli.
{
  "outcome" => "success",
  "response-headers" => {
    "operation-requires-reload" => true,
    "process-state" => "reload-required"
  }
}
Executing reload..
Silent Auth for Jboss Cli has been disabled
```

Check current the status of Silent Auth using:

```
./configureJbossCliSilentAuth.sh status
```

5. If you want to enable Silent Auth :

```
-bash-4.4$ ./configureJbossCliSilentAuth.sh on <jboss_cli_password>
```

Example output

```
Enabling Silent Auth for Jboss Cli.
{
  "outcome" => "success",
  "response-headers" => {
    "operation-requires-reload" => true,
    "process-state" => "reload-required"
  }
}
Executing reload..
Silent Auth for Jboss Cli has been enabled
```

Check the current status of Silent Auth using:

```
./configureJbossCliSilentAuth.sh status
```

RAMP Log Files

In this section:

- [Generate Log Files for Debugging](#)
- [List of Important RAMP Log Files](#)

This section lists some of the log files available in the Ribbon Application Management Platform (RAMP) system and the file locations (prescribed default locations at time of initial installation).

Generate Log Files for Debugging

To generate log files for debugging:

1. Log on to the RAMP CLI as the admin user.
2. Change to the insight user:

```
sudo su - insight
```

3. Use one of the following commands to archive the logs:
 - a. To archive the logs in the default directory:

```
/opt/sonus/ems/conf/archiveLogs.sh
```

The following message displays:

```
-bash-4.4$ ./archiveLogs.sh
```

This will create a tar file containing all log and configuration files associated with Insight EMS. Additionally, you will be able to enter comments below describing the problem or reason which has prompted you to create **this** archive file.

kafka topics - insight.node.change insight.node.info insight.config_node.node are used **for** collecting topic contents, **if** more topic is of interest, please add that in TOPICS_TO_COLLECT

Enter comments below. End comments with single "." character in **new** line

OR

- b. To archive the logs in a specific directory:

```
./archiveLogs.sh -d /opt/raid/
```

Note

-d lets you specify a destination directory for the archive tar ball. You are allowed to specify a different location beyond the default directory `/opt/sonus/ems` if the disk space is insufficient. The **-d** parameter is optional and defaults to `/opt/sonus/ems` when no directory is specified with **-d**.

Note

```
-bash-4.4$ ./archiveLogs.sh -d /opt/raid/
Using custom archive directory: /opt/raid/
```

This will create a tar file containing all log and configuration files associated with Insight EMS in /opt/raid/. You have the option to choose a different destination directory using the -d option.

Additionally, you will be able to enter comments below describing the problem or reason which has prompted you to create this archive file.

Kafka topics - insight.node.change insight.node.info insight.config_node.node are used for collecting topic contents, if more topic is of interest, please add that in TOPICS_TO_COLLECT

Enter comments below. End comments with single "." character in new line.

4. Enter a description for the log file. The following is an example:

```
The upgrade operation.
```

5. Press ENTER to move to the next line.
6. Enter a period (.) and press ENTER to save the logs. A message similar to the following displays:

```
#####
Creating a report on the Insight version information.
#####

#####
Gathering Linux Version Information.
#####

#####
Gathering Java Version Information.
#####

#####
Creating a snapshot of the system process table.
#####

#####
Capturing a list of the java processes and their arguments.
#####

#####
Creating a report on the system's free blocks on its disks.
#####

#####
Creating a report on the system's IP configuration
```



```
#####

#####
Creating a report on the system's processors.
#####

#####
Creating a report on the system's real memory size.
#####

#####
Creating a report on the system swap space.
#####

#####
Capturing the crontab.
#####

#####
Capturing ulimit settings.
#####

#####
Capturing output from dmesg.
#####

#####
Capturing Installed packages names
#####

#####
Capturing output from sysdef/sysctl.
#####
sysctl: reading key "net.ipv6.conf.all.stable_secret"
sysctl: reading key "net.ipv6.conf.bond0.stable_secret"
sysctl: reading key "net.ipv6.conf.default.stable_secret"
sysctl: reading key "net.ipv6.conf.eth0.stable_secret"
sysctl: reading key "net.ipv6.conf.eth1.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
#####

#####
Getting the User Activity entries from the database.
#####

#####
Creating logFiles-emssa-2020-11-20_114133.tar
#####

#####
About to gather some PM data from Kafka to write to logFiles-emssa-2020-11-20_1
14133.tar
```

```
#####

#####
Done gathering PM data from Kafka to write to logFiles-emssa-2020-11-20_114133.
tar

#####

#####
Adding /var/log/sa to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/kafka to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/sonus/unityexp/log to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/ems to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/dbaas to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/postgres to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/lsyncd to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
About to run archiveRootLogs.sh logFiles-emssa-2020-11-20_114133.tar

#####

#####
Adding /var/log/httpd to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/opensaf to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/session to logFiles-emssa-2020-11-20_114133.tar.
#####
```

```
#####
Adding /var/log/session_log to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/pgbouncer to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/repmgr to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/messages* to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding the output from journalctl to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/cloud-init.log to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/ntp.log to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /root/emsKickstartInstall.log and emsDBSetup.log to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /var/log/cron* to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding iptables and ip6tables output to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Done archiving the root owned logs.

#####

#####
Adding /etc/services to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
```

```

Adding PM LOGS /opt/sonus/pm/logs/* to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding PM DATA /opt/sonus/pm/data/* to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /opt/sonus/sonusComm/logs/* to logFiles-emssa-2020-11-20_114133.tar.
#####

#####
Adding /opt/sonus/sonusComm/blades/insight/conf/PersistedFailOverState.txt to
logFiles-emssa-2020-11-20_114133.tar.
Adding /opt/sonus/sonusComm/blades/insight/conf/PersistedProcList.txt to
logFiles-emssa-2020-11-20_114133.tar.
Adding /opt/sonus/sonusComm/blades/insight/conf/ProcMgmtList.xml to logFiles-
emssa-2020-11-20_114133.tar.
Adding /opt/sonus/sonusComm/conf/standaloneAgent.xml to logFiles-emssa-2020-11-
20_114133.tar.
#####

#####
Adding Node/ PM/ Licensing level report to logFiles-emssa-2020-11-20_114133.tar
.

#####
Adding POSTGRES LOGS /var/lib/pgsql/12/data/log/* to logFiles-emssa-2020-11-20_
114133.tar.
#####

#####
Adding CURRENT POSTGRES LOG /var/lib/pgsql/12/data/current_logfiles to
logFiles-emssa-2020-11-20_114133.tar.
#####

The archive file has been created and is located at:
/opt/sonus/ems/logFiles-emssa-2020-11-20_114133.tar.gz

-bash-4.2$

```

The log files are stored as a single `tar.gz` file at `/opt/sonus/ems` or at a customized location (as depicted in the above example `/opt/raid`) in the format `logFiles-<the RAMP hostname>-<timestamp>.tar.gz`

List of Important RAMP Log Files

The following logs are accessible via RAMP GUI under the Insight Administration option:

- User Activity Log—Records all user activity within RAMP server and PSX DB changes performed via the PSX Manager.
To view User Activity Log, refer to [Monitor User Activity](#).

- **System Activity Log**—Records error and warning messages regarding activity within the RAMP server. To view System Activity Log, refer to [System Activity Logging](#).
- **SSH Historical Log**—Provides detailed information about SSH events. There are six types of events logged. Depending upon the type of event, the system provides additional information pertaining to the log entry. In all cases the system begins the log entry with the day, date, and time of the event.
- **ems cli log**—Records results of executing PSX CLI scripts. Log files will have the format `ems_cli_log.<n>`, where <n> represents a sequence number from 1 to 5.

File name	Directory	Description
aggGSXSysDspResHighestUsageStat.log	/opt/sonus/pm/logs/	Contains information about the GSXSysDspResHighestUsageStat aggregation.
aggregator.log	/opt/sonus/pm/logs/	Contains information on PM Hourly Aggregator.
api_security_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains all of the RAMP API related authentication failures due to invalid or missing credentials.
authOutput.log	/opt/sonus/auth/logs/	Contains information on the abnormal events (exceptions) and information on the lifecycle of the Apache TomEE application server of the main Authentication & Authorization process.
authService.log	/opt/sonus/auth/logs/	Contains information related to the Authentication & Authorization startup.
auth_trace.log	/opt/sonus/auth/logs/	Contains logging information from the Authentication & Authorization. This log provides the most detailed information on the User/User Group/Role Management, tenant management, certificate management, realm management, and session management functionalities.
diagnose.log	/opt/sonus/auth/logs/	Contains information related to all the services exposed from Authentication & Authorization.
cm_trace_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains information on the agent managed device model framework (for configuring devices such as DSI).
converter.log	/opt/fm/logs/	Contains the logs for FM converter.

File name	Directory	Description
correlator.log	/opt/fm/logs/	Contains the logs for FM correlator.
correlator_schema_id.log	/opt/fm/logs/	Contains information on the fm correlator schema id.
cluster_aggregator.log	/opt/sonus/pm/logs/	Contains information on the PM cluster aggregator.
csrfguard.log	/opt/sonus/ems/ weblogic/ sonusEms/logs/sys	Contains all of anti-CSRF related logs (security).
Datahandler.log	/opt/sonus/pm/logs/	Contains the logs of PM Datahandler.
DataPurger.log	/opt/sonus/pm/logs/	Contains the logs of PM Data purging activity.
dbsink.log	/opt/fm/logs/	Contains the logs for FM dbsink
debezium_connect.log	/opt/fm/logs/	Contains the logs for FM debezium.
decoder_schema_id.log	/opt/fm/logs/	Contains information on the fm decoder schema id.
devMgmt_administration_trace_log	/opt/devMgmt/logs/	Contains the logs for DM administration.
devMgmt_auth_utils_trace_log	/opt/devMgmt/logs/	Contains the logs for DM authentication.
devMgmt_clustermgmtui_trace_log	/opt/devMgmt/logs/	Contains the logs for cluster management GUI operations.
devMgmt_dynamic_node_trace_log	/opt/devMgmt/logs/	Contains REST requests from dynamically registered nodes.
devMgmt_nodemgmt_trace_log	/opt/devMgmt/logs/	Contains REST requests from RAMP GUI and discovery.
devMgmt_inventory_service_trace_log	/opt/devMgmt/logs/	Contains the information on DM inventory service.
devMgmt_jpa_log	/opt/devMgmt/logs/	Contains the information of DM jpa logs

File name	Directory	Description
devMgmtOutput.log	/opt/devMgmt/logs/	Contains the information of DM service start/stop.
devMgmt_rg_service_trace_log	/opt/devMgmt/logs/	Contains the information for DM RG service.
devMgmt_utils_trace_log	/opt/devMgmt/logs/	Contains the DM utility trace logs.
di_trace_log	/opt/sonus/ems/weblogic /sonusEms/logs/sys	Contains information related to the DI (Device Inventory) feature. It contains details related to the hardware inventory collection process.
diagnose.log	/opt/fm/logs/	Contains the logs for FM diagnose.
dm_micro_service_logs	/opt/devMgmt/logs/	Contains information on every single reachability request which is set to the nodes to determine if they are up. Includes details on when the request was sent, which node name / IP address, and what the response was.
ems_ip_table_rules.log	/opt/sonus/ems/weblogic/ sonusEms/logs/sys	Contains the output of all of the iptables rules configuration.
ema_trace_log	/var/log/sonus/unityexp/log/ ema_trace.log	Contains logging information from the SBC Configuration Manager.
ems_cli_log	/opt/sonus/ems/weblogic/ sonusEms/logs/sys	Contains information on all CLI related activity performed on the RAMP.
ems_trace_log	/opt/sonus/ems/weblogic/ sonusEms/logs/sys	The most detailed log file about what is occurring in the main RAMP JBoss process. This is the same content which is reflected in the UI as the System Activity Log. The log includes details of the API request including version and revision of the cluster configurations.

File name	Directory	Description
emsapi_debug_log	/opt/sonus/ems/ weblogic/ sonusEms/logs/sys	Contains information related to the RAMP API deployment and other details related to operations that may fail. When DEBUG is enabled, the entire SOAP message is logged.
emsapi_prov_log	/opt/sonus/ems/ weblogic/ sonusEms/logs/sys	Contains information on all of the RAMP API operations that are performed including the user/IP performing the operation, what operation was invoked, and at what time the operation was invoked.
emsOutput.log	/opt/sonus/ems	Contains information about abnormal events (exceptions) as well as information about the startup of the JBoss application server for the main RAMP process.
emsRestart.log	/opt/sonus/ems/logs/ emsProcMgmt.log	Contains details about when the various RAMP processes are started and stopped.
exporter.log	/opt/fm/logs/	Contains the logs for FM exporter.
exportStatsPerNode.log	/opt/sonus/pm/logs/	Contains information on the statistics exported for PM perNode.
filter.log	/opt/fm/logs/	Contains the logs for FM filter.
fm.converter.log	/opt/fm/logs/	Contains start/stop information for the fm converter process.
fm.correlator.log	/opt/fm/logs/	Contains start/stop information for the fm correlator process.
fm.dbsink.log	/opt/fm/logs/	Contains start/stop information for the fm dbsink process.
fm.debezium_connect.log	/opt/fm/logs/	Contains start/stop information for the fm debezium_connect process.
fm.exporter.log	/opt/fm/logs/	Contains start/stop information for the fm exporter process.

File name	Directory	Description
fm.receiver.log	/opt/fm/logs/	Contains start/stop information for the fm receiver process.
fm.filter.log	/opt/fm/logs/	Contains start/stop information for the fm filter process.
fm.ossresync-agent.log	/opt/fm/logs/	Contains start/stop information for the fm ossresync-agent process.
fm.preprocessor.log	/opt/fm/logs/	Contains start/stop information for the fm preprocessor process.
fm.rest.log	/opt/fm/logs/	Contains start/stop information for the fm rest process.
fm.sequence-generator.log	/opt/fm/logs/	Contains start/stop information for the fm sequence-generator process.
fm.sequencer.log	/opt/fm/logs/	Contains start/stop information for the fm sequencer process.
genericNP_audit_log	/opt/sonus/ems/ weblogic/ sonusEms/logs/sys	Contains logging related to LNP/MNP.
generic_kafka_log	/opt/devMgmt/logs/	Contains the DM generic kafka logs
gsxUpgrade_trace_log	/opt/sonus/ems/ weblogic/ sonusEms/logs/sys	Contains logging information related to the GSX upgrade feature.
hibernate_log	/opt/sonus/ems/ weblogic/ sonusEms/logs/sys	Contains logging information related to Hibernate, the tool used to persist data to the RAMP database.
hornet_trace_log	/opt/sonus/ems/ weblogic/ sonusEms/logs/sys	Contains information related to the Netconf connections to the SBC.
kafka.log	/opt/sonus/ems/ weblogic/ sonusEms/logs/sys	Contains Kafka related logs.

File name	Directory	Description
li_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains logging related to the LI (Lawful Intercept) provisioning feature.
lm_diagnose_log	/opt/sonus/lm/logs/	Contains the logs for LM diagnose.
lm_trace_log	/opt/sonus/lm/logs/	Contains the logs for the complete LM service.
lmOutput.log	/opt/sonus/lm/logs/	Contains information about abnormal events (exceptions) as well as information about the startup of the Spring services for the LM.
lnp_trace_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains logging related to the LNP (Local Number Portability) feature.
logFiles- <EMS host name>- <timestamp in YYYY-MM-DD-HHMMSS format>.tar.gz Example: logFiles-emssa- 2020-11-20 _114133.tar.gz	/opt/sonus/ems	A tar.zip file which includes logs and PM yaml files for debugging the RAMP. Examples of the files included in logFiles*tar.zip: README emsMgmt userActivity.txt emsOutput.log ems_start.log emsRestart.log emsFM/logs/backupgc.log.current emsFM/logs/cert_mgmt.log emsFM/logs/debug.log emsFM/logs/fmOutput.log emsFM/logs/fm_receiver_audit emsFM/logs/fm_receiver_diagnosis emsFM/logs/fm_receiver_trace emsFM/logs/fm_receiver_trap_trace emsFM/logs/gc.log.0.current emsFM/logs/ossResyncMonitor.log emsFM/logs/ossTrapResync.log emsFM/logs/owl.log emsFM/logs/trapForwarderOutput.log emsFM/logs/trapMonitor.log emsFM/logs/trapMonitor.log.1 emsFM/logs/trapReceiverOutput.log emsFM/logs/trapResync.log weblogic/insight/log/backupgc.log.0 weblogic/insight/log/backupgc.log.2 weblogic/insight/log/backupgc.log.3

File name	Directory	Description
		weblogic/insight/log/backupgc.log.4 weblogic/insight/log/backupgc.log.current weblogic/insight/log/gc.log.0 weblogic/insight/log/gc.log.1 weblogic/insight/log/gc.log.2.current weblogic/insight/log/ localhost_access_log.2020-11-18 weblogic/insight/log/ localhost_access_log.2020-11-19 weblogic/insight/log/ localhost_access_log.2020-11-20 weblogic/insight/log/server.log weblogic/sonusEms/logs/sys/ api_security_log weblogic/sonusEms/logs/sys/cm_trace_log weblogic/sonusEms/logs/sys/csrfguard.log weblogic/sonusEms/logs/sys/ dashboard_log weblogic/sonusEms/logs/sys/di_trace_log weblogic/sonusEms/logs/sys/ ema_trace_log weblogic/sonusEms/logs/sys/ emsapi_debug_log weblogic/sonusEms/logs/sys/ emsapi_prov_log weblogic/sonusEms/logs/sys/ems_cli_log weblogic/sonusEms/logs/sys/ ems_iptable_rules.log weblogic/sonusEms/logs/sys/ ems_trace_log weblogic/sonusEms/logs/sys/fm_audit_log weblogic/sonusEms/logs/sys/ fmds_audit_log weblogic/sonusEms/logs/sys/ fmds_trace_log weblogic/sonusEms/logs/sys/fm_trace_log weblogic/sonusEms/logs/sys/ genericNP_audit_log weblogic/sonusEms/logs/sys/ gsxUpgrade_trace_log weblogic/sonusEms/logs/sys/ hibernate_log weblogic/sonusEms/logs/sys/ hornet_trace_log weblogic/sonusEms/logs/sys/kafka.log weblogic/sonusEms/logs/sys/kafka.log.1 weblogic/sonusEms/logs/sys/kafka.log.2 weblogic/sonusEms/logs/sys/kafka.log.3 weblogic/sonusEms/logs/sys/kafka.log.4 weblogic/sonusEms/logs/sys/kafka.log.5 weblogic/sonusEms/logs/sys/

File name	Directory	Description
		license_trace_log weblogic/sonusEms/logs/sys/li_log weblogic/sonusEms/logs/sys/lnp_trace_log weblogic/sonusEms/logs/sys/ mnp_syniverse_audit_log weblogic/sonusEms/logs/sys/ mnp_telcordia_audit_log weblogic/sonusEms/logs/sys/ mnp_trace_log weblogic/sonusEms/logs/sys/ nhr_trace_log weblogic/sonusEms/logs/sys/ openstack_trace_log weblogic/sonusEms/logs/sys/ partialConfigUpdate_log weblogic/sonusEms/logs/sys/ pm_diagnos_trace_log weblogic/sonusEms/logs/sys/ pm_trace_log weblogic/sonusEms/logs/sys/quartz_log weblogic/sonusEms/logs/sys/ reachability_audit_log weblogic/sonusEms/logs/sys/ sbcapi_prov_log weblogic/sonusEms/logs/sys/sgxapi_log weblogic/sonusEms/logs/sys/ smsapi_prov_log weblogic/sonusEms/logs/sys/ssh.log weblogic/sonusEms/logs/sys/tm_trace_log weblogic/sonusEms/logs/sys/tr746.log weblogic/sonusEms/logs/sys/ trapResync_log weblogic/sonusEms/logs/sys/ UA_18_11_2020_00_00.log weblogic/sonusEms/logs/sys/ UA_19_11_2020_00_00.log weblogic/sonusEms/logs/sys/ UA_20_11_2020_00_00.log weblogic/sonusEms/logs/sys/ual_trace_log weblogic/sonusEms/logs/sys/ vlan_trace_log weblogic/sonusEms/logs/psx/ callTraceEvents.log weblogic/sonusEms/logs/psx/ eventListener.log weblogic/sonusEms/data/sys/ ManagedAdax.txt weblogic/sonusEms/data/sys/ ManagedAsx.txt weblogic/sonusEms/data/sys/ ManagedDataNode.txt

File name	Directory	Description
		weblogic/sonusEms/data/sys/ ManagedDsc.txt weblogic/sonusEms/data/sys/ ManagedDsm.txt weblogic/sonusEms/data/sys/ ManagedDS.txt weblogic/sonusEms/data/sys/ ManagedFoundry.txt weblogic/sonusEms/data/sys/ ManagedGsx.txt weblogic/sonusEms/data/sys/ ManagedIDH.txt weblogic/sonusEms/data/sys/ ManagedInsight.txt weblogic/sonusEms/data/sys/ ManagedNetapps.txt weblogic/sonusEms/data/sys/ ManagedPsx.txt weblogic/sonusEms/data/sys/ ManagedRaid.txt weblogic/sonusEms/data/sys/ ManagedRiverstone.txt weblogic/sonusEms/data/sys/ ManagedSBCEDGE.txt weblogic/sonusEms/data/sys/ ManagedSBX1K.txt weblogic/sonusEms/data/sys/ ManagedSBX2K.txt weblogic/sonusEms/data/sys/ ManagedSBX5K.txt weblogic/sonusEms/data/sys/ ManagedSBX7K.txt weblogic/sonusEms/data/sys/ ManagedSgx4000.txt weblogic/sonusEms/data/sys/ ManagedSgx.txt weblogic/sonusEms/data/sys/ ManagedSLB.txt weblogic/sonusEms/data/sys/ ManagedSolaris.txt weblogic/sonusEms/data/sys/ ManagedSTI.txt weblogic/sonusEms/data/sys/ ManagedVnfm.txt weblogic/sonusEms/data/sys/ ManagedWSX.txt weblogic/sonusEms/data/sys/ SystemConfig.txt.keep weblogic/sonusEms/data/sys/ SystemConfig.txt weblogic/sonusEms/data/sys/

File name	Directory	Description
		apacheproxy_config.properties weblogic/sonusEms/data/sys/ apacheproxy_sbx_node.properties weblogic/sonusEms/data/sys/ apacheproxy_virtual_host.conf weblogic/sonusEms/data/sys/ apacheproxy_virtual_host_template.txt weblogic/sonusEms/data/sys/ emsapps_apacheproxy_virtual_host.conf emsFM/data/FmManagerProfile.txt emsFM/.fmsettings emsFM/server/faultmgmt/configuration/ standaloneFM.xml logs/AuthLog.log logs/cert_mgmt.log logs/changeDbPassword.log logs/changeInsightPassword.log logs/cloudEmsSetup.log logs/emsProcMgmt.log logs/ems_unbuffer.log logs/fileReplication.log logs/genKey.log logs/haEmsStart.log logs/haGeneric.log logs/kafkaStatus.log logs/kafkaStatus.log.1.gz logs/mirrormaker.log logs/orderdeployment.log log/emsFileDescriptorCount.log log/emsThreadCount.log conf/DM/DM_Version.properties weblogic/insight/conf/sonus-log4j.xml weblogic/insight/configuration/ standalone.xml JENKINS_BUILD_NO weblogic/sonusEms/data/sys/ DatabasePassword.txt weblogic/sonusEms/data/sys/ InsightPassword.txt weblogic/sonusEms/data/sys/ KeystorePassword.txt weblogic/sonusEms/data/sys/ PostgresPassword.txt weblogic/sonusEms/data/sys/.KF weblogic/sonusEms/data/sys/ ems.keystore weblogic/sonusEms/data/sys/ ems.keystore.seed weblogic/sonusEms/data/sys/ psxEventListener.properties weblogic/insight/ems/resources/properties/

File name	Directory	Description
		main/properties/ sonus-licmgr-config.xml etc/opensaf/imm.xml opt/sonus/userData.txt opt/sonus/userData.json opt/sonus/metadata.json opt/sonus/instanceData.json opt/sonus/network_data.json etc/sonus.conf MISC_LSYNC/.memsize .insight.pid .ems_pgsql_profile .bash_history kafka/confluent-5.3.1/logs/schema-registry.log kafka/confluent-5.3.1/logs/schemaRegistry.out pm_kafka_configuration.props SONUSDB_dir.txt opt/sonus/platform/logs/intel-common-platform-logging-2020-11-04-05-20-20.log opt/sonus/platform/logs/sethostname.log var/log/sa/ var/log/sa/sa15 var/log/sa/sa05 var/log/sa/sar13 var/log/sa/sar19 var/log/sa/sa12 var/log/sa/sa19 var/log/sa/sa07 var/log/sa/sa17 var/log/sa/sa09 var/log/sa/sar08 var/log/sa/sar10 var/log/sa/sa08 var/log/sa/sa18 var/log/sa/sar16 var/log/sa/sa16 var/log/sa/sar09 var/log/sa/sa11 var/log/sa/sar14 var/log/sa/sa13 var/log/sa/sar05 var/log/sa/sar15 var/log/sa/sa20 var/log/sa/sar11 var/log/sa/sar07 var/log/sa/sa06 var/log/sa/sar18 var/log/sa/sar06

File name	Directory	Description
		var/log/sa/sar12 var/log/sa/sa10 var/log/sa/sa14 var/log/sa/sar17 var/log/kafka/ var/log/kafka/server.log.1 var/log/kafka/connectStandalone.out.2.gz var/log/kafka/server.log.2.gz var/log/kafka/connectStandalone.out var/log/kafka/controller.log var/log/kafka/kafkaServer-gc.log.0.current var/log/kafka/controller.log.1 var/log/kafka/zookeeper.out.1 var/log/kafka/zookeeper.out.3.gz var/log/kafka/controller.log.2.gz var/log/kafka/connectStandalone.out.4.gz var/log/kafka/kafkaServer.out var/log/kafka/log-cleaner.log var/log/kafka/server.log var/log/kafka/state-change.log var/log/kafka/metadata-service.log var/log/kafka/connectStandalone.out.3.gz var/log/kafka/kafka-request.log var/log/kafka/zookeeper.out.4.gz var/log/kafka/kafka-authorizer.log var/log/kafka/server.log.4.gz var/log/kafka/zookeeper.out var/log/kafka/server.log.3.gz var/log/kafka/zookeeper.out.2.gz var/log/kafka/zookeeper-gc.log.0.current var/log/kafka/connectStandalone.out.1 var/log/sonus/unityexp/log/ var/log/sonus/unityexp/log/ema_trace.log var/log/sonus/unityexp/log/server.log var/log/sonus/unityexp/log/catalina.out var/log/ems/ var/log/ems/ opensaf_components_health.log.1.gz var/log/ems/ems_login.log var/log/ems/ems_user.log var/log/ems/ opensaf_components_health.log var/log/ems/ opensaf_components_health.log.2.gz var/log/ems/ opensaf_components_health.log.3.gz var/log/ems/opensaf_audits.log var/log/dbaas/ var/log/dbaas/dbaas_service.13815.log var/log/dbaas/dbaas_pw.11578.log var/log/dbaas/dbaas_service.10129.log

File name	Directory	Description
		var/log/dbaas/dbaas_service.4197.log var/log/dbaas/dbaas_pw.7377.log var/log/dbaas/dbaas_service.12363.log var/log/dbaas/dbaas_service.9203.log var/log/dbaas/ dbaas_config_hba.12747.log var/log/dbaas/dbaas_service.13533.log var/log/dbaas/dbaas_service.2580.log var/log/dbaas/dbaas_install.10042.log var/log/dbaas/dbaas_config_hba.9067.log var/log/dbaas/dbaas_service.13404.log var/log/dbaas/dbaas_service.11627.log var/log/dbaas/dbaas_monitor.log var/log/dbaas/dbaas_service.25855.log var/log/dbaas/dbaas_service.18063.log var/log/dbaas/dbaas_service.8850.log var/log/dbaas/dbaas_service.11196.log var/log/dbaas/dbaas_service.10355.log var/log/dbaas/dbaas_service.9143.log var/log/dbaas/createdb.log var/log/dbaas/dbaas_service.7229.log var/log/dbaas/dbaas_service.12787.log var/log/dbaas/ dbaas_rpm_post_install.10010.log var/log/dbaas/dbaas_service.4156.log var/log/dbaas/dbaas_config_hba.8993.log var/log/dbaas/dbaas_service.6989.log var/log/dbaas/ dbaas_config_hba.12706.log var/log/dbaas/dbaas_pw.20354.log var/log/dbaas/dbaas_service.6042.log var/log/dbaas/dbaas_service.719.log var/log/dbaas/dbaas_service.14283.log var/log/dbaas/dbaas_service.6908.log var/log/dbaas/dbaas_service.10812.log var/log/dbaas/dbaas_service.30897.log var/log/postgres/ var/log/postgres/CreatePGDB.log var/log/lsyncd/ var/log/httpd/ var/log/httpd/ssl_request_log var/log/httpd/access_log.2.gz var/log/httpd/error_log var/log/httpd/error_log.2.gz var/log/httpd/ssl_error_log.1 var/log/httpd/access_log.1 var/log/httpd/ssl_access_log var/log/httpd/ssl_error_log.2.gz var/log/httpd/ssl_error_log var/log/httpd/error_log.1 var/log/httpd/access_log

File name	Directory	Description
		var/log/opensaf/ var/log/opensaf/dtlog/ var/log/opensaf/nid.log var/log/opensaf/mds.log var/log/opensaf/saflog/ var/log/opensaf/saflog/ saLogSystem_20201105_123920.log var/log/opensaf/saflog/ saLogNotification.cfg var/log/opensaf/saflog/saLogSystem.cfg var/log/opensaf/saflog/ saLogAlarm_20201105_123920.log var/log/opensaf/saflog/saLogAlarm.cfg var/log/opensaf/saflog/ saLogNotification_20201105_123920.log var/log/session/ var/log/session/ admin_6335_20201115-230809_history.log var/log/session/ admin_17018_20201120-101936_history.log var/log/session_log/ var/log/session_log/admin/ var/log/session_log/admin/ admin_2020-11-14.tar.gz var/log/session_log/admin/ admin_2020-11-20.tar.gz var/log/session_log/admin/ admin_2020-11-18.tar.gz var/log/session_log/admin/ admin_2020-11-19.tar.gz var/log/session_log/admin/ admin_2020-11-16.tar.gz var/log/session_log/insight/ var/log/pgbouncer/ var/log/pgbouncer/pgbouncer.log var/log/pgbouncer/pgbouncer.log.1.gz var/log/pgbouncer/pgbouncer.log.2.gz var/log/repmgr/ var/log/messages var/log/messages.1.gz var/log/messages.2.gz var/log/journal.log var/log/cloud-init.log var/log/ntp.log root/emsKickstartInstall.log root/emsDBSetup.log var/log/cron var/log/cron.1.gz var/log/cron.2.gz

File name	Directory	Description
		iptables-save.out ip6tables-save.out services emsPM/ emsPM/cluster_aggregator.log emsPM/pm_jmx_collector_trace_log emsPM/Datahandler.log emsPM/pm_ftp_collector_trace_log emsPM/pm_snmp_collector_trace_log emsPM/pmOutput.log emsPM/aggregator.log emsPM/DataPurger.log emsPM/purgerStdrr.log emsPM/pm_diagnose_post.log emsPM/pm_datahandler_trace_log emsPM/pm_diagnose_log emsPM/ aggGSXSysDspResHighestUsageStat.log emsPM/processor.log emsPM/processorStdrr.log emsPM/persister.log emsPMdata/ emsPMdata/ PSX6000_Intel_SNMP_V13.02.00_0000. yaml emsPMdata/ SBX5K_Intel_SNMP_V08.01.00_0000.ya ml emsPMdata/ SBX7K_Intel_FTP_V08.01.00_0000.yaml emsPMdata/ SBX5K_Intel_SNMP_V09.02.00_0000.ya ml emsPMdata/ SBX5K_Intel_SNMP_V07.01.00_0000.ya ml emsPMdata/retentionperiod_properties emsPMdata/ SBX7K_Intel_FTP_V09.00.00_0000.yaml emsPMdata/ SBX5K_Intel_SNMP_V09.01.00_0000.ya ml emsPMdata/ GSX9000_Solaris_SNMP_V08.04.01_000 0.yaml emsPMdata/ PSX6000_Intel_FTP_V12.02.00_0000.ya ml emsPMdata/ PSX6000_Intel_SNMP_V07.03.04_0000. yaml

File name	Directory	Description
		emsPMdata/ GSX9000_Solaris_SNMP_V09.02.00_0000.yaml emsPMdata/ DSC_Intel_FTP_V16.00.00_0000.yaml emsPMdata/ GSX9000_Solaris_SNMP_V08.01.00_0000.yaml emsPMdata/ SBX5K_Intel_SNMP_V07.00.00_0000.yaml emsPMdata/ SBX7K_Intel_FTP_V08.02.00_0000.yaml emsPMdata/ PSX6000_Intel_SNMP_V07.01.02_0000.yaml emsPMdata/ PSX6000_Intel_SNMP_V08.01.00_0000.yaml emsPMdata/ GSX9000_Solaris_FTP_V09.00.00_0000.yaml emsPMdata/ PSX6000_Intel_SNMP_V07.03.07_0000.yaml emsPMdata/ SBX5K_Intel_FTP_V08.02.00_0000.yaml emsPMdata/ SBX5K_Intel_FTP_V05.00.04_0000.yaml emsPMdata/ SBX5K_Intel_SNMP_V05.01.02_0000.yaml emsPMdata/ SBX5K_Intel_FTP_V09.01.00_0000.yaml emsPMdata/ SBX5K_Intel_FTP_V05.01.00_0000.yaml emsPMdata/ SBX7K_Intel_FTP_V05.00.02_0000.yaml emsPMdata/ SBX5K_Intel_SNMP_V06.00.00_0000.yaml emsPMdata/ PSX6000_Intel_SNMP_V12.01.00_0000.yaml emsPMdata/ DSC_Intel_FTP_V14.00.00_0000.yaml emsPMdata/ PSX6000_Intel_FTP_V13.01.00_0000.yaml emsPMdata/ SBX5K_Intel_FTP_V07.00.00_0000.yaml

File name	Directory	Description
		emsPMdata/ SBX5K_Intel_SNMP_V09.00.00_0000.ya ml emsPMdata/ PSX6000_Intel_FTP_V11.02.00_0000.ya ml emsPMdata/ DSC_Intel_FTP_V18.00.00_0000.yaml emsPMdata/ SBX7K_Intel_FTP_V05.00.01_0000.yaml emsPMdata/ SBX5K_Intel_FTP_V06.01.00_0000.yaml emsPMdata/ SBX7K_Intel_FTP_V06.00.00_0000.yaml emsPMdata/ PSX6000_Intel_SNMP_V13.00.00_0000. yaml emsPMdata/ SBX7K_Intel_FTP_V06.01.00_0000.yaml emsPMdata/ PSX6000_Intel_SNMP_V12.02.01_0000. yaml emsPMdata/ PSX6000_Intel_SNMP_V08.02.01_0000. yaml emsPMdata/ SGX4000_Intel_SNMP_V07.03.05_0000. yaml emsPMdata/ PSX6000_Intel_FTP_V12.02.01_0000.ya ml emsPMdata/ GSX9000_Solaris_SNMP_V11.01.01_000 0.yaml emsPMdata/ SBX5K_Intel_FTP_V05.00.00_0000.yaml emsPMdata/ PSX6000_Intel_SNMP_V13.01.00_0000. yaml emsPMdata/ PSX6000_Intel_SNMP_V11.02.00_0000. yaml emsPMdata/ PSX6000_Intel_SNMP_V10.00.01_0000. yaml emsPMdata/ SBX5K_Intel_FTP_V05.00.01_0000.yaml emsPMdata/ DSC_Intel_FTP_V15.01.00_0000.yaml emsPMdata/ GSX9000_Solaris_FTP_V08.03.00_0000.

File name	Directory	Description
		yaml emsPMdata/ SBX7K_Lintel_FTP_V06.02.00_0000.yaml emsPMdata/ SBX5K_Lintel_FTP_V08.01.00_0000.yaml emsPMdata/ INSIGHT_Lintel_FTP_V13.00.00_0000.yaml emsPMdata/ SBX5K_Lintel_SNMP_V06.01.00_0000.yaml emsPMdata/ GSX9000_Solaris_SNMP_V10.01.00_0000.yaml emsPMdata/ SBX7K_Lintel_FTP_V04.02.04_0000.yaml emsPMdata/ SLB_Lintel_FTP_V09.02.00_0000.yaml emsPMdata/ SLB_Lintel_FTP_V09.01.00_0000.yaml emsPMdata/ PSX6000_Lintel_SNMP_V11.00.00_0000.yaml emsPMdata/ SBX5K_Lintel_FTP_V06.02.00_0000.yaml emsPMdata/ SBX7K_Lintel_FTP_V09.01.00_0000.yaml emsPMdata/mdjson/ emsPMdata/mdjson/ SGX4000_metadata.json emsPMdata/mdjson/ INSIGHT_metadata.json emsPMdata/mdjson/ SBX7K_metadata.json emsPMdata/mdjson/EDGE_metadata.json emsPMdata/mdjson/ SBX5K_metadata.json emsPMdata/mdjson/DSC_metadata.json emsPMdata/mdjson/DSI_metadata.json emsPMdata/mdjson/ PSX6000_metadata.json emsPMdata/mdjson/ GSX9000_metadata.json emsPMdata/mdjson/SLB_metadata.json emsPMdata/ SBX7K_Lintel_FTP_V04.00.00_0000.yaml emsPMdata/ SBX7K_Lintel_FTP_V08.00.00_0000.yaml emsPMdata/ INSIGHT_Lintel_SNMP_V07.01.00_0000.yaml

File name	Directory	Description
		emsPMdata/ SBX5K_Lintel_SNMP_V08.02.00_0000.ya ml emsPMdata/ PSX6000_Lintel_SNMP_V07.01.00_0000. yaml emsPMdata/ PSX6000_Lintel_SNMP_V07.02.02_0000. yaml emsPMdata/ SBX7K_Lintel_FTP_V05.01.00_0000.yaml emsPMdata/ SBX7K_Lintel_FTP_V05.01.02_0000.yaml emsPMdata/ GSX9000_Solaris_FTP_V11.01.01_0000.y aml emsPMdata/ SBX5K_Lintel_FTP_V05.00.05_0000.yaml emsPMdata/ SBX5K_Lintel_SNMP_V05.00.01_0000.ya ml emsPMdata/ SBX5K_Lintel_FTP_V08.00.00_0000.yaml emsPMdata/ PSX6000_Lintel_FTP_V11.00.00_0000.ya ml emsPMdata/ DSI_Solaris_SNMP_V07.00.00_0000.yaml emsPMdata/ PSX6000_Lintel_FTP_V12.01.00_0000.ya ml emsPMdata/ SBX7K_Lintel_FTP_V07.01.00_0000.yaml emsPMdata/exportColOrder.properties emsPMdata/ SBX5K_Lintel_FTP_V05.01.02_0000.yaml emsPMdata/ SGX4000_Lintel_SNMP_V09.00.00_0000. yaml emsPMdata/ SBX7K_Lintel_FTP_V05.00.00_0000.yaml emsPMdata/ DSI_Lintel_SNMP_V07.00.00_0000.yaml emsPMdata/ PSX6000_Lintel_SNMP_V09.01.00_0000. yaml emsPMdata/ PSX6000_Lintel_SNMP_V07.02.00_0000. yaml emsPMdata/ SGX4000_Lintel_SNMP_V07.03.00_0000.

File name	Directory	Description
		yaml emsPMdata/ SBX5K_Intel_SNMP_V05.00.04_0000.ya ml emsPMdata/ SBX5K_Intel_FTP_V07.01.00_0000.yaml emsPMdata/ DSC_Intel_FTP_V15.02.00_0000.yaml emsPMdata/ EDGE_Intel_SNMP_V03.00.00_0000.ya ml emsPMdata/pm_config.properties emsPMdata/ PSX6000_Intel_SNMP_V10.03.00_0000. yaml emsPMdata/ DSC_Intel_FTP_V17.00.00_0000.yaml emsPMdata/ SBX5K_Intel_SNMP_V05.00.00_0000.ya ml emsPMdata/ GSX9000_Solaris_FTP_V10.01.00_0000. yaml emsPMdata/ PSX6000_Intel_SNMP_V10.02.00_0000. yaml emsPMdata/ PSX6000_Intel_SNMP_V07.03.05_0000. yaml emsPMdata/ SBX5K_Intel_FTP_V06.00.00_0000.yaml emsPMdata/ PSX6000_Intel_SNMP_V08.03.00_0000. yaml emsPMdata/ PSX6000_Intel_SNMP_V07.03.00_0000. yaml emsPMdata/ GSX9000_Solaris_SNMP_V08.00.01_000 0.yaml emsPMdata/parquet_files.txt emsPMdata/ PSX6000_Intel_FTP_V13.02.00_0000.ya ml emsPMdata/ SBX7K_Intel_FTP_V04.01.00_0000.yaml emsPMdata/ PSX6000_Intel_SNMP_V07.02.03_0000. yaml emsPMdata/ GSX9000_Solaris_FTP_V09.02.00_0000.

File name	Directory	Description
		yaml emsPMdata/ SBX5K_Lintel_FTP_V05.00.02_0000.yaml emsPMdata/ PSX6000_Lintel_SNMP_V09.02.00_0000. yaml emsPMdata/ GSX9000_Solaris_FTP_V09.00.02_0000. yaml emsPMdata/ SBX7K_Lintel_FTP_V04.02.00_0000.yaml emsPMdata/ GSX9000_Solaris_SNMP_V09.00.00_000 0.yaml emsPMdata/ GSX9000_Solaris_FTP_V08.04.01_0000. yaml emsPMdata/ SBX5K_Lintel_FTP_V09.00.00_0000.yaml emsPMdata/ SBX5K_Lintel_SNMP_V05.00.05_0000.ya ml emsPMdata/ DSC_Lintel_FTP_V19.00.00_0000.yaml emsPMdata/ PSX6000_Solaris_SNMP_V11.02.00_000 0.yaml emsPMdata/ PSX6000_Lintel_SNMP_V10.00.00_0000. yaml emsPMdata/ GSX9000_Solaris_SNMP_V08.03.00_000 0.yaml emsPMdata/ SBX7K_Lintel_FTP_V05.00.04_0000.yaml emsPMdata/ SBX5K_Lintel_FTP_V09.02.00_0000.yaml emsPMdata/ PSX6000_Lintel_FTP_V13.00.00_0000.ya ml emsPMdata/ SBX5K_Lintel_SNMP_V06.02.00_0000.ya ml emsPMdata/ PSX6000_Lintel_SNMP_V12.02.00_0000. yaml emsPMdata/ PSX6000_Lintel_SNMP_V09.03.00_0000. yaml emsPMdata/ SBX7K_Lintel_FTP_V07.00.00_0000.yaml

File name	Directory	Description
		emsPMdata/ SBX5K_Lintel_SNMP_V07.02.00_0000.yaml emsPMdata/ SBX5K_Lintel_FTP_V07.02.00_0000.yaml emsPMdata/ SLB_Lintel_FTP_V08.01.00_0000.yaml emsPMdata/ SBX5K_Lintel_SNMP_V08.00.00_0000.yaml emsPMdata/ SBX7K_Lintel_FTP_V09.02.00_0000.yaml emsPMdata/ PSX6000_Lintel_SNMP_V09.00.00_0000.yaml emsPMdata/ PSX6000_Lintel_FTP_V10.03.00_0000.yaml emsPMdata/ SGX4000_Lintel_SNMP_V07.03.01_0000.yaml emsPMdata/ SBX5K_Lintel_SNMP_V05.01.00_0000.yaml emsPMdata/ SBX7K_Lintel_FTP_V05.00.05_0000.yaml emsPMdata/ SBX7K_Lintel_FTP_V07.02.00_0000.yaml sonusComm/logs/ sonusComm/logs/ resources.stats.15_minute_data.audit sonusComm/logs/ resources.stats.30_minute_data.audit sonusComm/logs/agent_trace_log sonusComm/logs/ resources.stats.5_minute_data.audit sonusComm/logs/standalone.log sonusComm/logs/proc_mgmt.log sonusComm/logs/ resources.stats.15_minute_data.audit.1 sonusComm/logs/application.stats.audit sonusComm/logs/sonusAgent.log sonusComm/logs/ha_audit_log sonusComm/logs/agent.messaging.audit.1 sonusComm/logs/EventMgrLog.audit sonusComm/logs/resources.stats.audit.1 sonusComm/logs/console.log sonusComm/logs/agent.messaging.audit sonusComm/logs/EventMgr.audit sonusComm/logs/access.audit sonusComm/logs/

File name	Directory	Description
		resources.stats.daily_data.audit sonusComm/logs/ha_failover.log sonusComm/logs/sonusAgent.log.1 sonusComm/logs/ resources.stats.60_minute_data.audit sonusComm/logs/resources.stats.audit sonusComm/logs/discover_config.error sonusComm/logs/application.monitor.audit sonusComm/logs/application.stats.audit.1 sonusComm/blades/insight/conf/ PersistedFailOverState.txt sonusComm/blades/insight/conf/ ProcMgmtList.xml sonusComm/conf/standaloneAgent.xml omnibus/db/SONUSDB/ master_store_0.chk omnibus/db/SONUSDB/ master_store_0.log omnibus/db/SONUSDB/ master_store_1.chk omnibus/db/SONUSDB/ master_store_1.log omnibus/db/SONUSDB/master_store.tab omnibus/db/SONUSDB/table_store_0.chk omnibus/db/SONUSDB/table_store_0.log omnibus/db/SONUSDB/table_store_1.chk omnibus/db/SONUSDB/table_store_1.log omnibus/db/SONUSDB/table_store.tab omnibus/etc/nco_config.props omnibus/etc/nco_confpack.props omnibus/etc/nco_dbinit.props omnibus/etc/NCO_PROXY.props omnibus/etc/SONUSDB.props omnibus/etc/nco_pa.conf omnibus/log/inst_err_log omnibus/log/NCOMS_audit_file.log omnibus/log/SONUSDB_audit_file.log omnibus/log/SONUSDB.log omnibus/log/SONUSDB.log_old omnibus/log/ SONUSDB_profiler_report.log1 omnibus/log/SONUSDB_trigger_stats.log1 omnibus/log/SONUSDB_trigger_stats.log2 omnibus/log/sonustrap.log omnibus/log/sonustrap.stats omnibus/log/sonustrap.trace omnibus/var/SONUSDB.pid omnibus/var/ nco_p_sonustrap.SONUSDB.alerts.status. def omnibus/probes/linux3x86/

File name	Directory	Description
		sonustrap.classes omnibus/probes/linux3x86/ sonustrap.clearing omnibus/probes/linux3x86/ sonustrap.dynamic omnibus/probes/linux3x86/sonustrap.help omnibus/probes/linux3x86/ sonustrap.labels omnibus/probes/linux3x86/ sonustrap.names omnibus/probes/linux3x86/ sonustrap.nodes omnibus/probes/linux3x86/ sonustrap.objids omnibus/probes/linux3x86/ sonustrap.props omnibus/probes/linux3x86/ sonustrap.raid_sun omnibus/probes/linux3x86/sonustrap.rules omnibus/probes/linux3x86/ sonustrap.severity omnibus/probes/linux3x86/ sonustrap.summaries omnibus/probes/linux3x86/ sonustrap.trunkgroups omnibus/probes/linux3x86/ user_defined.classes omnibus/probes/linux3x86/ user_defined.severity omnibus/probes/linux3x86/ user_defined.summaries omnibus/RELEASE_ID opt/sonus/ems/conf/PM_Report.txt log/postgresql-Wed.logcurrent_logfiles
mnpsyniverse_audit_log	/opt/sonus/ems/ weblogic/ sonusEms/logs/sys	Contains information on the count of MNP Syniverse messages received calculated every 5 minutes. If you are not using the feature, the log file will just contain entries with all 0s.
mnptelcordia_audit_log	/opt/sonus/ems/ weblogic/ sonusEms/logs/sys	Contains information on the count of MNP Telcordia messages received calculated every 5 minutes. If you are not using the feature, the log file will just contain entries with all 0s.

File name	Directory	Description
mnp_trace_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains logs related to the MNP feature.
nhr_trace_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains logs related to the Health Reports feature.
oss-resync-agent.log	/opt/fm/logs/	Contains the logs for FM oss-resync-agent.
oss_resync_stats.log	/opt/fm/logs/	Contains the logs for FM oss_resync_stats.
partialConfigUpdate_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains information related to the SBC partial configuration update feature.
persister.log	/opt/sonus/pm/logs/	Contains information related to the PM persister.
pm_administration_trace_log	/opt/sonus/pm/logs/	Contains information related to the PM administration service.
pm_copier_service_trace_log	/opt/sonus/pm/logs/	Contains information related to the copier service.
pm_datahandler_trace_log	/opt/sonus/pm/logs/	Contains information related to the PM datahandler service.
pm_diagnose_log	/opt/sonus/pm/logs/	Contains the logs for PM diagnose.
pm_diagnose_post_aggregator.log	/opt/sonus/pm/logs/	Contains the logs for PM aggregator diagnose.
pm_diagnose_post_exporter.log	/opt/sonus/pm/logs/	Contains the logs for PM exporter diagnose.
pm_diagnose_post_processor.log	/opt/sonus/pm/logs/	Contains the logs for PM post processor diagnose.
pm_exporter_trace_log	/opt/sonus/pm/logs/	Contains the logs for the PM exporter service.

File name	Directory	Description
pm_jmx_collector_trace_log	/opt/sonus/pm/logs/	Contains the logs for PM JMX Collection.
pm_pmc_trace_log	/opt/sonus/pm/logs/	Contains information about enabling/disabling a profile on a node.
pm_reports_trace_log	/opt/sonus/pm/logs/	Contains information about PM reports that are generated in UI.
pm_retention_trace_log	/opt/sonus/pm/logs/	Contains information related to the retention service.
pm_snmp_collector_trace_log	/opt/sonus/pm/logs/	Contains the logs for PM SNMP collection.
pm_sftp_collector_trace_log	/opt/sonus/pm/logs/	Contains the logs for PM SFTP collection.
pm_thresholder_trace_log	/opt/sonus/pm/logs/	Contains information about thresholder service.
pm_uai_log	/opt/sonus/pm/logs/	Contains the PM user activity logs.
pmOutput.log	/opt/sonus/pm/logs/	Contains info about PM microservices status.
preprocessor.log	/opt/fm/logs/	Contains information related to the FM preprocessor service.
processor.log	/opt/sonus/pm/logs/	Contains information related to the PM processor service.
processorStdrr.log	/opt/sonus/pm/logs/	Contains information about any errors/warns that are generated by python scripts.
preprocessor_schema_id.log	/opt/fm/logs/	Contains information related to the FM preprocessor schema_id.
purgerStdrr.log	/opt/sonus/pm/logs/	Contains the logs for PM purger error information.

File name	Directory	Description
quartz_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains information on the Quartz scheduler (used to schedule various job/tasks within the main RAMP JBoss instance).
ramp_trap.log	/opt/fm/logs/	Contains the logs for RAMP's traps.
reachability_audit_log	/opt/devMgmt/logs/	Contains the reachability audit information.
reachability_kafka_log	/opt/devMgmt/logs/	Contains the reachability kafka information.
reachability_quartz_log	/opt/devMgmt/logs/	Contains the reachability quartz information.
reachability_trace_log	/opt/devMgmt/logs/	Contains the reachability trace information.
receiver.log	/opt/fm/logs/	Contains information related to the FM receiver service.
sbcapi_prov_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains information on all of the SBC API operations that are performed including the user/IP performing the operation, what operation was invoked, and at what time the operation was invoked.
sequence-generator.log	/opt/fm/logs/	Contains information related to FM sequence-generator service.
sequencer.log	/opt/fm/logs/	Contains the logs for FM sequencer service.
sequencer_schema_id.log	/opt/fm/logs/	Contains the fm sequencer schema_id information.
sgxapi_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains information on all of the SGX API operations that are performed including the user/IP performing the operation, what operation was invoked, and at what time the operation was invoked.

File name	Directory	Description
ssh.log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains logging information related to SSH connections to other nodes. This typically just contains errors indicating failures when connecting.
ssh_log	/opt/devMgmt/logs/	Contains the DM ssh log information.
tm_trace_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains information about Traffic Management related operations.
tr746.log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains logging information related to the TR746 interface.
trap.log	/opt/fm/logs/	Contains the trap log information.
trap_stats.log	/opt/fm/logs/	Contains the trap stats log information.
fm_microservice_logs and other fm_micro_service_logs	/opt/fm/logs/	Contains information related to the trap resync feature.
UA_ <MM_DD_YYYY_hh_mm > .log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains the exported logs from the User Activity Log from the database at the given date and time that are specified in the filename.
ual_trace_log	/opt/sonus/auth/logs	Contains logging related to the User Activity Logger task which generates the UA_<MM_DD_YY_hh_mm>.log files.
vlan_trace_log	/opt/sonus/ems/weblogic/sonusEms/logs/sys	Contains information related to the VLAN feature.

Reset Admin Password for Jboss CLI

Reset the Admin password for the JBoss CLI using the Ribbon Application Management Platform (RAMP).

Prerequisite

RAMP is up and running.

Start

Use this procedure to reset the admin password for the JBoss CLI.

1. Log on to the RAMP as the `Insight` user. For more information, refer to [Log onto the RAMP CLI](#).
2. Use the `help` command to see the password hints on resetting the admin password for JBoss CLI:

```
/opt/rbbn/ems/conf/security/resetJbossCliAdminPass.sh -help
```

Output

The password must satisfy the following requirements:

It must contain at least 8 characters.

It must contain at least one alphabetic character.

It must contain at least one digit.

It must contain at least one non-alphanumeric symbol.

3. Reset the JBoss CLI admin password:

```
/opt/rbbn/ems/conf/security/resetJbossCliAdminPass.sh
```

At the prompts, enter and then re-enter the new password:

Output

```
-bash-4.4$ /opt/rbbn/ems/conf/security/resetJbossCliAdminPass.sh
```

```
Enter new Password :
```

```
Re-enter the Password :
```

```
Password Reset completed successfully.
```

Managing the NTP Server

In this section:

- [Add Multiple NTP Servers for RAMP](#)
- [Synchronize RAMP with the NTP Server](#)

Add Multiple NTP Servers for RAMP

To add multiple NTP IP addresses for Ribbon Application Management Platform (RAMP):

1. Log on to the RAMP CLI as the admin user.
2. Change to the root user:

```
sudo su -
```

3. Edit `/etc/chrony.conf`.
4. Append below lines at the end of the file:

```
server <NTP IP addresses 1> iburst  
restrict <NTP IP addresses 1> iburst
```

The following is an example:

```
server 10.128.254.67 iburst  
server 10.128.254.68 iburst
```

5. Save the file.
6. Restart NTP service:

```
systemctl restart chronyd
```

7. Run the `chronyc sources` to see the updated status.

Synchronize RAMP with the NTP Server

Your Unix/Linux administrator must synchronize Ribbon Application Management Platform (RAMP) and all network elements in the deployed network to the same NTP server. Synchronizing ensures that the timestamps in the RAMP logs are consistent with the timestamps on the other network elements. Failure to do so could also introduce error into certain statistics, most notably the Trunk Group performance statistics.

Note

If you elect to synchronize with more than one NTP server, you must ensure that the NTP servers are also synchronized. Conflicting time information from multiple NTP servers may cause RAMP system errors.

Start

Perform the following procedure to configure the NTP server in Linux. Ensure all nodes are set in the NTP server. By default, the GSX has the NTP server set.

1. SSH to RAMP as the admin user.
2. Change to root user:

```
sudo su -
```

3. Enter the following command to stop the NTP service:

```
# systemctl stop chronyd.service
```

- Using the vi editor, update `/etc/chrony.conf` file and add the NTP server IP address `<ntp_server_ip> iburst`.
For example:

```
# server 10.128.144.50 iburst
```

- Enter the command `chronyd -q server <ntp_server_ip> iburst` to synchronize the RAMP with the NTP server:
For example:

```
# chronyd -q server 10.128.144.50 iburst
```

- Start the NTP server:

```
# systemctl start chronyd
```

- After 10 seconds run the following command to ensure you are able to ping the NTP server:

```
chronyc tracking
```

Or

```
chronyc sources
```

Managing Redundancy

In this section:

- [Check Database and File Replication Status](#)
- [Change the Role of a Node in RAMP GR](#)
- [Reconfigure a Standby Node in RAMP GR](#)
- [Tear Down RAMP GR](#)
- [Replace a Node in RAMP GR](#)

A geographically redundant (GR) deployment on Ribbon Application Management Platform(RAMP) begins as two RAMP standalone instances at different geographical locations that you configure to work together in a GR fashion. The RAMP instance at one of the GR sites functions as a "source" or active RAMP and the other functions as a "target" or standby RAMP instance. GR configuration can be run on either standalone RAMP instance; the instance on which you configure GR becomes the source RAMP. Refer to [Configuring RAMP GR](#).

After GR is configured, there is constant replication of data from the source RAMP to the target RAMP. If the source RAMP goes down, you can perform a failover from the target RAMP instance. Similarly, you can also do a switchover and change the source and target roles. If necessary, you can also teardown the GR setup and resume having two standalone RAMP instances. If one instance fails, you have the option to replace it with a new instance.

As an alternative to initiating manual switchovers, RAMP also supports a deployment model that enables automatic switchover between GR instances. To enable automatic switchover, you must deploy three additional

VMs, each running an instance of etcd. The etcd instances continually monitor whether they are able to communicate with the RAMP instances and use that information to function as arbitrators that determine which RAMP instance should be active. A switchover occurs automatically when a majority of the etcd instances determine that the current active instance is no longer reachable. Refer to [Configuring RAMP GR with Automatic Switchover Enabled](#) for more information on switchover processing, the resources required to implement automatic switchover, and how to deploy etcd.

In a RAMP GR setup, the target instance monitors the source and raises the following alarms to a configured Operations Support Systems (OSS) when necessary:

- `sonusEmsV2NodeUnreachableNotification` target RAMP sends the alarm to OSS when the source RAMP is down.
- `sonusEmsV2NodeReachableNotification` target RAMP sends the alarm to OSS when the source RAMP is up and running.

Check Database and File Replication Status

To check the database and file replication status in a geographically redundant (GR) Ribbon Application Management Platform (RAMP) deployment, enter the following command on the active device as the `root` user:

```
/opt/sonus/ems/conf/RDSyncStatus.sh
```

The following is a sample output:

```
[2022-06-20 15:51:52 root@sanrampr1: /home/admin ]# /opt/sonus/ems/conf/RDSyncStatus.sh

This node is configured as a PHYSICAL replication PRIMARY.

Downstream Node Name | Node IP | State | Local LSN | Remote LSN | Lag(MB)
-----+-----+-----+-----+-----+-----
+-----+-----+
sanrampr2 | 172.19.52.66 | streaming | 0/5939B558 | 0/5939B558 | 0.000

-----
Component | Status
-----
PM | Sync completed
Inventory Report | Sync completed
SBC Image | Sync completed
```

Change the Role of a Node in RAMP GR

Use the following procedure to change the role of a Ribbon Application Management Platform (RAMP) node from active (source) to standby (target), or vice versa, in a geographically redundant (GR) deployment.

Note

The SBC Edge nodes take approximately 5 to 18 minutes to display the online status on the devices page after they are relocated.

You can change the role of a **RAMP** node (relocate) in either of the following scenarios. The scenario determines on which node to run the procedure.

- Switchover: Planned relocate operation on a node.
- Failover: Unplanned relocation operation as the other node failed.

Start

1. Accomplish one of the following role changes:
 - a. Failover: SSH to the **RAMP** standby **RAMP** node as insight user.
 - b. Switchover: SSH to the **RAMP** active **RAMP** node as insight user.
2. Change to the insight user:

```
sudo su - insight
```

3. Enter the following command:

```
nohup ./emsMgmt relocateGR &
```

Note

This command runs the process in the background.

Note

If you relocate a node for a failover, when the failed active node is restored it resumes operation as active, which can result in two active GR nodes. To resolve this issue, follow the procedure [Reconfigure a Standby Node in RAMP GR](#).

Note

Use the `tail -f nohup.out` command to see the progress.

Reconfigure a Standby Node in RAMP GR

In a Ribbon Application Management Platform (RAMP) geographically redundant (GR) deployment, if the active (source) instance is down, you can promote the standby (target) instance to be the active instance. However, when the active instance recovers, it comes up as active. This results in two active instances (dual-active condition) simultaneously.

To avoid the dual-active condition, use the following procedure to reconfigure the recovered active instance to be the standby instance.

1. SSH to the recovered RAMP active instance as the `admin` user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the `admin` user.
2. Change to insight user:

```
sudo su - insight
```

3. Enter the following command:

```
/opt/sonus/ems/emsMgmt grStandby
```

4. Exit the insight user session:

```
exit
```

5. Change to root user:

```
sudo su -
```

6. Reboot the node:

```
reboot
```

Tear Down RAMP GR

Use the following procedure to split a Ribbon Application Management Platform (RAMP) Geographically Redundancy (GR) deployment into two standalone instances for troubleshooting (recovery) or upgrade purposes. The RAMP GR devices are configured to work as an active (source) and standby (target) pair. When you tear down the GR configuration, these devices become standalone instances.

Prerequisites

Two healthy RAMP nodes, up and running.

Start

1. SSH to the RAMP active instance in the GR pair as the `admin` user. To access RAMP CLI as the `admin` user, refer to [Log onto the RAMP CLI](#).
2. Change to root user:

```
sudo su -
```

Note

Enter the Admin password if JITC is enabled.

Please enter Password of admin user **for** all nodes ->

3. Enter the following command:

Note

Use `-h` to list the options available when you run the `./RDtearDown.sh` command.

For example,

```
/etc/sonus/RDtearDown.sh -h
```

- h Show help information
- f FreshStart the RDteardown, instead of resuming from previous point of failure
- r RemoveSite with id or Node ID
- p Force Remove Remote Node or teardown when Gr is in bad state , when Remote Node is not Reachable/Down

```
/etc/sonus/RDtearDown.sh
```

The following message displays:

```
....  
Node 1 will be excluded because it is the local node  
Please enter the numeric site number to be removed ->
```

4. Enter the node number which you want to remove. For example, 2. The following message displays:

```
.....  
[12:08:27] Redundancy cluster node removal completed.  
Please check log file: /var/log/ems/RDtearDown.sh.7393.log
```

If the teardown process is interrupted and you resume `RDtearDown.sh`, RAMP shows the following message:

```
Record showing the <script name> script was being executed and was not
completed.
Do you want to resume the operation from the previous point of failure (yes|
no)?.
```

Perform one of the following:

- Enter "yes" to resume the operation from the point of failure.
- Enter "no" to execute the script again. RAMP shows the following message:

```
Do you want to proceed with a fresh new operation (yes|no)? ->
```

Perform one the following:

- Enter "yes" to execute the script.
- Enter "no" to terminate the session.

Note

The new certificates are generated for the target RAMP containing the CN and SAN details of the target.

Replace a Node in RAMP GR

If a Ribbon Application Management Platform (RAMP) instance in a geographically redundant (GR) deployment becomes corrupted, you can replace the corrupted RAMP instance with a new RAMP instance.

If an active GR instance fails but is not corrupted and could recover, manually promote the standby instance to the active role. Refer to [Change the Role of a Node in RAMP GR](#).

Start

1. Delete the corrupted RAMP instance.
2. Install a new RAMP instance with the same IP address and hostname of the corrupted instance.
3. Log onto the new RAMP instance through CLI as the `admin` user.
4. Change to the `root` user:

```
sudo su - root
```

5. Find the `_node<number>_id` of the corrupted node:

```
cat /etc/rd.conf
```

6. Execute the following command:


```
/etc/sonus/RDupdateNode.sh <_node_id of the corrupted node>
```

The following is an example:

```
/etc/sonus/RDupdateNode.sh 02
```

The following is a sample output:

```
....
Please enter Password of admin user for all nodes (press ENTER if not needed) ->
```

7. Enter the password of the admin user. The following is a sample output:

```
.....
Do you want to proceed with updating this node (yes|no)?
```

8. Enter "yes". The following is a sample output:

```
....
You can login as insight user and invoke "./emsMgmt status" to check the cluster status.
```

If the replacement process is interrupted and you resume `RDupdateNode . sh` , RAMP shows the following message:

```
Record showing the <script name> script was being executed and was not completed.
Do you want to resume the operation from the previous point of failure (yes|no)?.
```

Perform one of the following:

- Enter "yes" to resume the operation from the point of failure.
- Enter "no" to execute the script again. The RAMP shows the following message:

```
Do you want to proceed with a fresh new operation (yes|no)? ->
```

Perform one the following:

- Enter "yes" to execute the script.
- Enter "no" to terminate the session.

Managing Resources

In this section:

- [Manage Resources for RAMP on KVM](#)

- [Change CPU Count in the RAMP on KVM Using CLI](#)
- [Change Memory Allocation in the RAMP on KVM Using CLI](#)
- [Manage Resources for RAMP on OpenStack](#)
 - [Detach a Cinder Volume from an Instance](#)
 - [Delete Stack](#)
 - [Delete a Cinder Volume](#)
 - [Recovering RAMP from Nova Compute Failure](#)
- [Manage Resources for RAMP on VMware ESXi](#)
 - [Change CPU Count in RAMP on VMware](#)
 - [Change Memory Allocation in RAMP on VMware](#)

Manage Resources for RAMP on KVM

In this section:

- [Change CPU Count in the RAMP on KVM Using CLI](#)
- [Change Memory Allocation in the RAMP on KVM Using CLI](#)

Change CPU Count in the RAMP on KVM Using CLI

Use this procedure to change the CPU count for a Ribbon Application Management Platform (RAMP) device deployed on KVM.

To change the CPU count:

1. Log onto the KVM host as root user.
2. List all the instances and select the instance from the list that you want to update.

```
virsh list --all
```

Sample output:

Id	Name	State

44	ems-image-based-install	running

3. Shut down the VM:

```
virsh shutdown <vm_name>
```

Sample output:

```
virsh shutdown  ems-image-based-install

Domain ems-image-based-install is being shutdown
```

4. Verify whether the VM is shut off:

```
virsh dominfo ems-image-based-install | grep State
```

Sample output:

```
State: shut off
```

5. Check the CPU count in the VM instance:

```
virsh dominfo <vm_name> | grep CPU
```

Sample output:

```
virsh dominfo ems-image-based-install | grep CPU
CPU(s):      4
```

6. Check whether topology is defined:

```
virsh dumpxml <vm_name> | grep -C 1 cores
```

Sample output that indicates a predefined topology (4 vCPUs):

```
<cpu>
  <topology sockets='1' cores='2' threads='2' />
</cpu>
```

Note

If there is no predefined topology, no output is displayed.

7. If sample output exists indicating a predefined topology, perform the following sub-step. Otherwise, skip to step 8.
 - Edit the XML and edit your <CPU> topology depending on your requirement and change the VCPU allocation to match.

If you have defined the topology (socket, core and threads), edit both the maximum count and the topology.

```
virsh edit <vm_name>
```

Sample output (6 cores):

```
virsh edit ems-image-based-install
```

```
Domain ems-image-based-install XML configuration edited.
```

```
-----
<cpu>
  <topology sockets='1' cores='3' threads='2' />
</cpu>
```

8. Update the CPU count:

```
virsh setvcpus <vm_name> <vcpu_count> --config --maximum
virsh setvcpus <vm_name> <vcpu_count> --config
```

Sample output (changing CPU count to 6):

```
virsh setvcpus ems-image-based-install 6 --config --maximum

virsh setvcpus ems-image-based-install 6 --config

virsh dominfo ems-image-based-install | grep CPU
CPU(s):          6
```

Change Memory Allocation in the RAMP on KVM Using CLI

Use the following procedure to change the memory allocation for a Ribbon Application Management Platform (RAMP) device deployed on KVM.

1. Log onto the KVM host as the root user.
2. List all the instances and select the instance from the list that you want to change.

```
virsh list --all
```

Sample output:

```
virsh list --all

  Id      Name                                State
  -----
  44      ems-image-based-install              running
```

3. Shut down the RAMP VM:

```
virsh shutdown <vm_name>
```

Sample output:

```
virsh shutdown ems-image-based-install
```

```
Domain ems-image-based-install is being shutdown
```

4. Verify whether the VM is shut off:

```
virsh dominfo ems-image-based-install | grep State
```

Sample output:

```
State:          shut off
```

5. Check the memory allocation of the instance.

```
virsh dominfo <vm_name> | grep memory
```

Sample output:

```
virsh dominfo ems-image-based-install | grep memory
Max memory:    66969600 KiB
Used memory:    66969600 KiB
```

6. Change the memory allocation:

```
virsh setmaxmem <vm_name> <memsize> --config
virsh setmem <vm_name> <memsize> --config
```

Sample output:

```
virsh setmaxmem ems-image-based-install 73400320 --config

virsh setmem ems-image-based-install 73400320 --config

virsh dominfo ems-image-based-install | grep memory
Max memory:    73400320 KiB
Used memory:    73400320 KiB
```

Manage Resources for RAMP on OpenStack

In this section:

- [Detach a Cinder Volume from an Instance](#)
- [Delete Stack](#)
- [Delete a Cinder Volume](#)
- [Recovering RAMP from Nova Compute Failure](#)

Detach a Cinder Volume from an Instance

You can detach a cinder volume that is associated with an instance of Ribbon Application Management Platform (RAMP).

To detach a cinder volume:

1. Log onto the OpenStack Dashboard GUI.
2. Click **Project -> Volumes**.
3. Select the cinder volume to detach.
4. From the **Actions** drop-down list, select **Manage Attachments**.
The **Manage Volume Attachments** dialog box is displayed.
5. Click **Detach Volume**.
You are prompted to confirm.

Once a cinder volume is no longer attached you can delete the cinder volume if appropriate, refer to [Delete a Cinder Volume](#).

Delete Stack

When you upgrade Ribbon Application Management Platform (RAMP) on OpenStack, you must delete the instance's stack as part of the upgrade process. When you delete a stack on OpenStack, this removes the instance that was spawned using the respective stack and also disassociates any attached Cinder volume. However, the Cinder volume is not deleted; it can be reused.

Start

1. Log onto the OpenStack Dashboard GUI.
2. Click **Project > Compute > Instances**.
From the **Instances** list, note down the floating IP associated with the instance you plan to delete. The IP address will be released when you delete the stack.
3. Click **Project > Compute > Volumes**. Note down the Cinder volume associated with the RAMP instance. This Cinder volume is disassociated from the instance when you delete the stack, but the data persists as long as the Cinder volume is not deleted. If you delete the Cinder volume, the data is lost.
4. Click **Project > Orchestration > Stacks**. Select the RAMP stack for the instance you want to terminate and click **Delete Stacks**.
5. Confirm the deletion when prompted.
6. Click **Project > Compute > Instances** and verify that the RAMP instance is no longer listed.
7. Click **Project > Compute > Volumes** and verify that the Cinder volume is disassociated from the RAMP instance.
8. (Optional) If you are no longer planning to reuse the data on the Cinder volume, you can delete the Cinder volume. Select the Cinder volume and click **Delete Volumes** to delete the Cinder volume.
9. Confirm the deletion when prompted.

Deleting the Cinder volume results in loss of backup data.

10. Check if the Cinder volume is deleted from the **Volumes** list.

Delete a Cinder Volume

You can delete a cinder volume that is not attached to any instance to save disk space.

To delete a cinder volume:

1. Log onto the OpenStack Dashboard GUI.

2. Click **Project -> Volumes**.
3. Select a cinder volume to delete and confirm when prompted.
4. Click **Delete Volumes**.
The cinder volume is deleted.

Recovering RAMP from Nova Compute Failure

Use this procedure to recover (evacuate) a Ribbon Application Management Platform (RAMP) instance from a failed Nova Compute node.

Prerequisites

- RAMP is running on a multi-host OpenStack setup with multiple Compute nodes running.

For this procedure, assume Compute nodes A and B are running in Openstack and you want to evacuate the RAMP instance from node A (which is now down) to node B.

Start

1. Verify that Compute node A is down by entering the following command:

```
nova service-list
```

2. Evacuate the instance by entering the following command.

```
nova evacuate <instance name> <compute B>
```

The RAMP instance on Compute node A is moved to the second host (Compute node B).

3. Verify if RAMP and all its processes are running on Compute node B. Refer to [Check RAMP Status](#).
4. Log onto the RAMP GUI and verify that the RAMP GUI displays.

Manage Resources for RAMP on VMware ESXi

In this section:

- [Change CPU Count in RAMP on VMware](#)
- [Change Memory Allocation in RAMP on VMware](#)

This section covers managing system resources for Ribbon Application Management Platform (RAMP) on VMware ESXi.

Change CPU Count in RAMP on VMware

Use the following procedure to change the CPU count for a Ribbon Application Management Platform (RAMP) device deployed on VMware ESXi.

To change the number of CPUs:

1. Enter the VMware host machine IP address in your web browser and log in as the `root` user.
2. In the left navigation pane under **Virtual Machines**, select the VM you want to configure.
3. Power off the VM.
4. Click **Edit**.
The **Edit settings** window opens for the selected VM.
5. In **CPU**, select a CPU count as needed.
6. Click **Save**.
7. Power on the VM.

Change Memory Allocation in RAMP on VMware

Use the following procedure to change the memory allocation for a Ribbon Application Management Platform (RAMP) device deployed on VMware ESXi.

To change the memory allocation:

1. Enter the VMware host machine IP address in your web browser and log in as the `root` user.
2. In the left navigation pane under **Virtual Machines**, select the VM you want to configure.
3. Power off the VM.
4. Click **Edit**.
The **Edit settings** window opens for the selected VM.
5. In **Memory**, enter the new memory allocation quantity.
6. Click **Save**.
7. Power on the VM.

Managing Secure Communications

In this section:

- [Secure Login to the RAMP GUI](#)
 - [Generate a Certificate Request for the RAMP GUI](#)
 - [Import Trusted Certificates for the RAMP GUI](#)
 - [Import Previously Generated TLS Certificate](#)
- [Secure Communication Between RAMP and Devices](#)
 - [Generate Certificate Request for Agent](#)
 - [Import Certificates for Agent](#)
 - [Add an Intermediate Certificate in SSL Handshake](#)
 - [Renew RAMP Certificates](#)
- [Enable Key-Based Authentication for SSH](#)
 - [Obtain the RAMP SSH Keys](#)

Secure Login to the RAMP GUI

Related articles:

- [Generate a Certificate Request for the RAMP GUI](#)
- [Import Trusted Certificates for the RAMP GUI](#)
- [Import Previously Generated TLS Certificate](#)

Hypertext Transfer Protocol Secure (HTTPS) is used to secure logins to the Ribbon Application Management Platform (RAMP) GUI. RAMP requires an SSL certificate in order to use HTTPS. Installing an SSL certificate will prevent errors and warnings on the RAMP login page. Without a certificate, the RAMP login page will show a “Not Secure” warning.

HTTPS is enabled by default. However, the default site certificate on RAMP is only a demo version. You can use this demo certificate only for testing and training.

To support production use, Ribbon recommends that you obtain a site certificate for each RAMP device from a trusted Certificate Authority (CA) designated by your organization. System administrators must coordinate closely with their chosen CA. For more information, refer to <https://docs.oracle.com/javase/8/docs/technotes/guides/security/cert3.html>.

For RAMP GR, repeat the procedures to secure the communication on both the active and standby devices.

To get help on certificate commands, enter the following command when logged in as the insight user. Refer to [Log onto the RAMP CLI](#) for information on accessing RAMP as the insight user.

```
/opt/sonus/ems/conf/cert/bin/manageCert -h
```

Logs for RAMP GUI certificate commands are available at `/opt/sonus/ems/logs/cert_mgmt.log`.

Workflow – Secure Login to RAMP GUI

Step	Action
1	Generate a Certificate Request for the RAMP GUI
2	Import Trusted Certificates for the RAMP GUI

Generate a Certificate Request for the RAMP GUI

The Ribbon Application Management Platform (RAMP) requires an SSL certificate for users to log into the GUI securely. SSL certificates are issued by a Certificate Authority (CA). To obtain certificates, the RAMP administrator needs to send a certificate service request (CSR) to a CA.

This section covers generating a CSR.

Prerequisites

SSH credentials for the RAMP `insight` user.

Note

The RAMP supports certificates with key size ranging from 2048 to 4096 bits. If you migrate data to a new RAMP system, any certificates with a key size less than 2048 are not restored. You must generate a new certificate using the following procedure.

Start

1. Access RAMP as the `insight` user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the `insight` user.
2. Perform one of the following:
 - Create a configuration file with an IP address for CSR generation:

```
/opt/sonus/ems/conf/cert/bin/manageCert config-csr
```

Example output:

```
-bash-4.4$ /opt/sonus/ems/conf/cert/bin/manageCert config-csr
Generating certificate request template config file for EMS site IP ...
Successfully created template config file: /opt/sonus/ems/conf/cert/conf/
request-cert.cfg

Please fill in rest of the details here before using this config file for
certificate request generation.
-bash-4.4$
```

OR

- Create a configuration file without an IP address for certificate request generation:

```
/opt/sonus/ems/conf/cert/bin/manageCert config-csr -e
```

Example Output:

```
-bash-4.4$ /opt/sonus/ems/conf/cert/bin/manageCert config-csr -e
Generating certificate request template config file for EMS site IP ...
Successfully created template config file: /opt/sonus/ems/conf/cert/conf/
request-cert.cfg

Please fill in rest of the details here before using this config file for
certificate request generation.
-bash-4.4$
```

3. Edit the certificate request configuration file. No commas are allowed for the key values.

Parameter	Description	Example	Mandatory (M)/ Optional (O)
cert.FQDN	The Fully Qualified Domain Name (FQDN) of the RAMP site. For example: If you plan to access your RAMP site from a browser using <code>https://emshost.yourdomain.com</code>, enter the FQDN value as "emshost.yourdomain.com". The FQDN must contain only alphanumeric characters, hyphens, and periods. Note Ensure you have created a DNS entry for the FQDN to resolve it correctly to the RAMP IP address.	emsha1.rbbn.com	M
cert.IP	Note Do not enter any value for the <code>cert.IP</code> parameter if you have generated the certificate service request (CSR) without an IP address. RAMP's IP address.	10.155.75.200	M
cert.CN	The Common Name (CN) for the hostname.	ribbon.com	O
cert.organizationUnit	The department or division in the organization.	Purchasing	O
cert.organizationName	The organization name.	Ribbon Communications	O
cert.localityName	The locality name.	Westford	O
cert.stateName	The state or province name.	Massachusetts	O

Parameter	Description	Example	Mandatory (M)/ Optional (O)
cert.country	The two-letter country code.	US	O
cert.rsa.keySize	The RSA encryption key length (in bits) to generate an RSA key pair during CSR generation. ◦ 2048 bits – For general-purpose encryption and secure communication to provide a good balance between security and performance. ◦ 4096 bits – (Default) This offers the highest level of protection for highly sensitive data and long-term security requirements, but it may require more computational resources.	4096	M

4. Save the file.

Sample request-cert.cfg details

```
-bash-4.4$ cat /opt/sonus/ems/conf/cert/conf/request-cert.cfg
#
# Fully Qualified Domain Name (FQDN) of the EMS site.
#
# For example:
#   If you plan to access your EMS site from the browser as: https://
#   emshost.yourdomain.com
#   Then the FQDN value should be: emshost.yourdomain.com
#
# Please make sure that you have created a DNS entry for this FQDN so that it
# resolves correctly to the IP: 10.54.141.76
#
# RSA Key Bit Size. Min Size Supported=2048, Max Size Supported=4096
cert.rsa.keySize=4096

# Create/Update the value below as appropriate
cert.FQDN=venus2ems.$dnsSearchPath

# IP address of EMS site (Well-known/virtual IP in case of EMS HA) - you usually
# would not need to change this
cert.IP=10.54.141.76

# Common Name (CN) for the hostname, e.g., "sonusnet.com"
cert.CN=
```

```
# Small organization (e.g., department or division) name, e.g., "Purchasing."
cert.organizationUnit=

# Large organization (Company) name, e.g., "ABCSystems."
cert.organizationName=

# Locality (city) name, e.g., "Palo Alto"
cert.localityName=

# Full State or province name, e.g., "California."
cert.stateName=

# Two-letter country code, e.g., "US"
cert.country=

-bash-4.4$
```

5. Generate the CSR. The validity of a certificate is set to 1 year (365 days) by default. Change the certificate validity (in days) using the `-v` argument. Perform one of the following.
 - Generate a CSR without an IP address. The example requests certificates with 30 days of validity.

```
/opt/sonus/ems/conf/cert/bin/manageCert gen-csr -v 30 -e
```

Example output:

```
-bash-4.4$ /opt/sonus/ems/conf/cert/bin/manageCert gen-csr -v 30 -e

Creating a certificate requestwith thee following settings:

Fully Qualified Domain Name .. ....: rampdemo.rbbn.com
RSA Key Bit Size.....: 4096 bits
Certificate validity period .....: 30 days

Do you want to proceed? [y|n]: y

Starting certificate request generation with validity of 30 days.
Creating working copy of keystore file ems.keystore as ems.keystore.staging...
Removing old key first from keystore...
Generating key pairs...
Generating certificate request file /opt/sonus/ems/conf/cert/conf/
rampDemo_SonusEMS.csr...
Successfully completed certificate request file generation.

Please use the following file to request a new site certificate:
/opt/sonus/ems/conf/cert/conf/rampDemo_SonusEMS.csr
-bash-4.4$
```

- Generate a CSR with an IP address. The example requests certificates with 30 days of validity.

```
/opt/sonus/ems/conf/cert/bin/manageCert gen-csr -v 30
```

6. When a prompt "Do you want to proceed? [y|n]:" displays, enter "y". The CSR file is generated.
7. **Verify the CSR before sending it to the CA:**

```
/opt/sonus/ems/conf/cert/bin/manageCert verify-csr
```

Example Output:

```
-bash-4.4$ /opt/sonus/ems/conf/cert/bin/manageCert verify-csr
Printing contents of certificate request file: /opt/sonus/ems/conf/cert/conf/
rampDemo_SonusEMS.csr

PKCS #10 Certificate Request (Version 1.0)
Subject: CN=rampdemo.rbbn.com, OU=SVT, O=Ribbon Communications, L=Bangalore,
ST=Karnataka, C=IN
Format: X.509
Public Key: 4096-bit RSA key
Signature algorithm: SHA256withRSA

Extension Request:

#1: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: rampdemo.rbbn.com
  IPAddress: 10.34.146.32
]

#2: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E2 25 27 EB A3 A6 85 56  0C 30 13 C8 91 AE 89 E4  .%'....V.0.....
0010: 2B FC 8D 04                      +...
]
]
```

- a. **Check the hostname:**

```
hostname
```

- b. (Optional) Remove ^M characters from the CSR:

```
dos2unix /opt/sonus/ems/conf/cert/conf/<hostname>_SonusEMS.csr
```

- c. **Check the contents in the CSR:**

```
cat /opt/sonus/ems/conf/cert/conf/<hostname>_SonusEMS.csr
```

8. Send the CSR to a CA and follow the procedure to obtain certificates. After obtaining the certificates, import them to RAMP. Refer to [Import Trusted Certificates for the RAMP GUI](#) for additional information.

Troubleshooting:

1. Refer to the log file `/opt/sonus/ems/logs/cert_mgmt.log`.
2. For detail logging, edit the file `/opt/sonus/ems/conf/cert/conf/log4j.xml`.

Import Trusted Certificates for the RAMP GUI

Use this procedure to import trusted certificates obtained from a Certificate Authority (CA) to Ribbon Application Management Platform (RAMP). You will usually receive two or three certificate files (root, intermediate, and site) from a request. The 'site' certificate is for the RAMP host, and can have a dependency on an 'intermediate' certificate or 'root' certificate, or both. The intermediate certificate is optional.

RAMP certificates in X.509 format may have different extensions (.cer, .crt, .pem, .der, and so on). The certificates will work if they are in PEM (ASCII) or DER (Binary) format, irrespective of the file extension.

Prerequisites

- A [Certificate Request](#) for the RAMP GUI exists.

Start

1. Copy the certificates to the RAMP host in the directory `/tmp`.
2. Access RAMP as the root user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the root user.
3. Add permissions for the insight user to access the certificate files:

```
chown insight:insight /tmp/ramp-site.cer
chown insight:insight /tmp/verisign-root-ca.cer
chown insight:insight /tmp/verisign-intermediate-ca.cer
```

4. Change to insight user:

```
sudo su - insight
```

5. Verify certificates are available in RAMP:

```
ls -ltr /tmp/*.cer
```

The following is an example of three files containing certificates:

```
-rw-r--r--. 1 insight insight 1854 Jan 11 19:49 /tmp/ramp-site.cer
-rw-r--r--. 1 insight insight 1964 Jan 11 19:50 /tmp/verisign-intermediate-ca.cer
```

```
-rw-r--r--. 1 insight insight 1566 Jan 11 19:50 /tmp/verisign-root-ca.cer
```

6. Add the paths for certificates into the `conf/import-cert.cfg` config file, starting with the root certificate. You can keep any alias (key) for the root and intermediate certificates in the config file, but the alias has to be 'insight' for the site certificate (reply for the certificate request sent to CA earlier). If the root and intermediate certificates have been imported, they do not need to be specified again in the config file. The site certificate (with the 'insight' alias name) is required. The following is an example of the config file after the update:

```
cat /opt/sonus/ems/conf/cert/conf/import-cert.cfg
# Specify the certificates to be imported, in ORDER, starting with the root CA
cert,
# and ending with the cert for Insight EMS site (with alias name 'insight').
#
# In case you have received a single cert file which already contains the
certificate chain, then specify
# that file path with the alias name 'insight'
#
# Entries should be in the following format: <alias>=<path to certificate file>
# For example:
#
# verisign-root-ca=/opt/sonus/ems/tmp/verisignca.crt
# geotrust-intermediate-ca=/opt/sonus/ems/tmp/geotrust-intermediate.pem
# insight=/opt/sonus/ems/tmp/sonusems.der
#
# Only X.509 format certificates are supported, certificates in other formats (e.g
PKCS #7) need to be
# manually converted to X.509 first before being used by this script.
#
# Certificate files need to be encoded in either 'PEM' (ascii) or 'DER' (binary),
extension doesn't matter.
# Alias names are case-insensitive and should be unique.
# Alias for the Insight EMS site certificate should be 'insight' (without quotes)
insight=/tmp/ramp-site.crt
verisign-root-ca=/tmp/verisign-root-ca.crt
```

```
grep -v "#" /opt/sonus/ems/conf/cert/conf/import-cert.cfg | grep =
verisign-root-ca=/tmp/verisign-root-ca.cer
verisign-intermediate-ca=/tmp/verisign-intermediate-ca.cer
insight=/tmp/ramp-site.cer
```

7. If the certificates from the CA are obtained in a bundle format, for example as a PKCS 12 (.pfx file) or PKCS 7 (.p7b file), manually split the file into individual PEM encoded certificate files and then add the paths to those files in the `import-cert.cfg` file. For example, if you receive a .p7b file, you can convert it into a PEM-encoded file as follows (change input and output file names appropriately):

```
$ openssl pkcs7 -print_certs -in /tmp/incerts.p7b -out /tmp/outcerts.cer
```

8. Open the output file and place each BEGIN CERTIFICATE and END CERTIFICATE block (including those two lines), and place them in separate files.

9. Place the paths for these separate files into the *import-cert.cfg* file.
10. Verify the certificates before importing them to the **RAMP** keystore. It is recommended that you verify the certificate fingerprints with the fingerprints provided by the CA. You can also specify the alias name using the `-n` argument to view the certificate for only that alias name, as specified in the *import-cert.cfg* configuration file. If no arguments are provided, all the certificates mentioned in the configuration file are displayed. For example, enter the following command to view and verify the certificate details for only the **insight** alias (site certificate):

```
/opt/sonus/ems/conf/cert/bin/manageCert verify-cert -n insight
```

Sample output

```
$ /opt/sonus/ems/conf/cert/bin/manageCert verify-cert -n insight
Validating certificate config
Printing contents of single certificate file /tmp/ramp-site.crt with alias name
'insight'...

Owner: CN=rampdemo.rbbn.com, OU=SVT, O=Ribbon Communications, L=Bangalore,
ST=Karnataka, C=IN
Issuer: EMAILADDRESS=rampdemo@rbbn.com, CN=rampdemo, OU=SVT, O=Ribbon
Communications, L=Bangalore, ST=Karnataka, C=In
Serial number: 8e18e2396ac1f625fc2cd4c7a44bd09f09926d5
Valid from: Fri Feb 23 16:05:55 IST 2024 until: Mon Jul 07 16:05:55 IST 2025
Certificate fingerprints:
    SHA1: 4A:AE:A1:3D:20:85:25:E7:0A:67:A9:07:90:1F:E0:14:65:88:51:FF
    SHA256: C2:CC:94:4B:10:1C:53:F2:E9:80:A5:00:D7:A8:96:BF:8A:43:8D:A0:2C:C9
:EB:99:C9:35:BF:86:E7:B6:0F:3A
Signature algorithm name: SHA256WITHRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 1
```

11. Import certificate:

```
/opt/sonus/ems/conf/cert/bin/manageCert import-cert
```

Sample output

```
Starting certificate imports
Validating certificate config
Importing following certificates:
  1. verisign-root-ca [file: /tmp/verisign-root-ca.cer]
  2. verisign-intermediate-ca [file: /tmp/verisign-intermediate-ca.cer]
  3. insight [file: /tmp/ramp-site.cer]
Do you want to proceed? [y|n]:
```

12. Enter "y". The certificates are imported.

```
/opt/sonus/ems/conf/cert/bin/manageCert import-cert
Starting certificate imports
Validating certificate config

Importing following certificates:

  1. insight [file: /tmp/ramp-site.crt]
  2. verisign-root-ca [file: /tmp/verisign-root-ca.crt]

Do you want to proceed? [y|n]: y

Starting import of CA certificate file /tmp/verisign-root-ca.crt with alias name
'verisign-root-ca'
Checking whether certificate 'verisign-root-ca' file /tmp/verisign-root-ca.crt is
in DER format
Certificate not in DER format, checking if in PEM format
Certificate in PEM format, will be converting to DER format
Saving original file as .orig
Starting conversion to DER format
Verifying DER encoded certificate...
Successfully converted certificate file /tmp/verisign-root-ca.crt to DER format
Completed format check for certificate 'verisign-root-ca'
Deleting old certificate 'verisign-root-ca', if any, from keystore before adding
new one
Importing CA certificate 'verisign-root-ca'
Successfully imported CA certificate file /tmp/verisign-root-ca.crt with alias
name 'verisign-root-ca'
Starting import of SITE certificate file /tmp/ramp-site.crt with alias name
'insight'
Checking whether certificate 'insight' file /tmp/ramp-site.crt is in DER format
Certificate not in DER format, checking if in PEM format
Certificate in PEM format, will be converting to DER format
Saving original file as .orig
Starting conversion to DER format
Verifying DER encoded certificate...
Successfully converted certificate file /tmp/ramp-site.crt to DER format
Completed format check for certificate 'insight'
Importing SITE certificate 'insight'
Successfully imported SITE certificate file /tmp/ramp-site.crt with alias name
'insight'
Finally deleting the demo certificate if present.
Finally deleting the demo certificate if present.
Finally updating the keystore in use...
Setting up keys for Apache proxy
Extracting key...
Successfully extracted key, now converting key to PKCS#12 format
Successfully created PKCS#12 file, now converting to PEM format.
Removing passphrase from PEM file.
Setting file permissions
Completed setting up keys for Apache proxy.
```

Completed certificate imports

13. Stop the RAMP. For more information, refer to [How to Start and Stop RAMP](#).
14. Start the RAMP. For more information, refer to [How to Start and Stop RAMP](#).
15. Confirm whether certificates are imported to RAMP:

```
/opt/sonus/ems/conf/cert/bin/manageCert show-cert -n <alias name>
```

Viewing the 'insight' (site) certificate example

```
/opt/sonus/ems/conf/cert/bin/manageCert show-cert -n insight
```

You can now securely log on to the RAMP GUI.

Import Previously Generated TLS Certificate

The Ribbon Application Management Platform (RAMP) allows you to install a certificate by raising a request even from a third-party system. You need not go to RAMP, run the script, and generate the request. RAMP allows you to import certificates whose Certificate Signing Request (CSR) is raised from a different system.

Prerequisites

RAMP supports PKCS#12 (.p12) format.

PKCS#12 is a binary format for storing the server certificate, intermediate certificates, and private key in one file. This conveniently packages both the certificate and private key together simplifying the import process.

PKCS#12 files are particularly suited for importing certificates into your application due to the following reasons:

- It includes both a certificate and a private key, making it easier to manage and import all necessary certificate components.
- It provides enhanced security to ensure that sensitive data is securely handled during the import process.
- Its simplicity helps in streamlining the import process and reduces the risk of errors.

Perform the following to import SSL/TLS certificates into the RAMP application's keystore.

These certificates are generated using external tools or processes rather than through the application's built-in CSR generation procedure.

Start

1. Download the PKCS#12 File.

- a. Obtain the certificates provided by the Certificate Authority (CA).

It will typically be in the form of a .p12, includes the private key, the public certificate, and potentially intermediate certificates.

- b. Download this PKCS#12 file from the CA or the IT department.
2. Transfer the PKCS#12 File to RAMP.
 - a. Upload the .p12 file to the /tmp directory on the application server.
 - b. Ensure that the file has the correct ownership and permissions
 - i. Owner: insight
 - ii. Group: insight
 - iii. Permissions: 640
 - c. Execute the command.

```
chown insight:insight /tmp/yourfile.p12
```

- d. Execute the command.

```
chmod 640 /tmp/yourfile.p12
```

3. Import the PKCS#12 File into the RAMP's Keystore.
 - a. Login to RAMP and run the Import Script as 'insight' user.
 - b. Execute the command.

```
/opt/sonus/ems/conf/cert/bin/manageCert import-pkcs12 -p /tmp/yourfile.p12
```

- c. The script will securely prompt for the PKCS#12 password/passphrase ensuring that the password is not displayed in the console during entry.
 - d. Enter the password to complete the import.
4. Extract/Split certificates from the downloaded PKCS#12 file.
 - a. Use OpenSSL command to extract the certificates.

Example

```
openssl pkcs12 -in /tmp/yourfile.p12 -nokeys -out /tmp/all_certs.pem
```

- b. After extracting the certificates, manually split and save each certificate into its own file.

The extracted certificates need to be saved individually, with clear naming to distinguish between the root, intermediate, and site certificates. Each certificate begins with -----BEGIN CERTIFICATE----- and ends with -----END CERTIFICATE-----.

- c. Open the `all_certs.pem` file in a text editor, and for each certificate block.
 - i. Save the root certificate as `root.cer`.
 - ii. Save the intermediate certificate (if present) as `intermediate.cer`.
 - iii. Save the site certificate as `site.cer`.
5. Prepare for the final Import.
 - a. To import the certificates, refer to [Import Trusted Certificates for the RAMP GUI](#).

Secure Communication Between RAMP and Devices

Related articles:

- [Generate Certificate Request for Agent](#)
- [Import Certificates for Agent](#)
- [Add an Intermediate Certificate in SSL Handshake](#)
- [Renew RAMP Certificates](#)

Hypertext Transfer Protocol Secure (HTTPS) is used on Ribbon Application Management Platform (RAMP) for secure communication with registered devices. HTTPS is enabled by default, but the agent on RAMP requires an SSL certificate in order to use HTTPS. However, the default site certificate on RAMP is only a demo version. You can use the demo certificate only for testing and training.

To support production use, Ribbon recommends you obtain a site certificate for each RAMP device from a trusted Certificate Authority (CA) designated by your organization. System administrators must coordinate closely with their chosen CA. For more information, refer to <https://docs.oracle.com/javase/8/docs/technotes/guides/security/cert3.html>.

For RAMP GR deployments, repeat procedures to secure to communication on both the active and standby devices.

To get help on certificate commands, enter the following command as the insight user. Refer to [Log onto the RAMP CLI](#) for information on accessing RAMP as the insight user.

```
/opt/sonus/sonusComm/conf/cert/bin/manageCert -h
```

Logs for RAMP agent commands are available at `/opt/sonus/sonusComm/logs/cert_mgmt.log`.

Workflow – Secure Communication Between RAMP and Devices

Step	Action
1	Generate Certificate Request for Agent
2	Import Certificates for Agent
3	(Optional) Add an Intermediate Certificate in SSL Handshake

For managing certificates for PSX Agent, refer to [PSX Agent Certificate Management](#).

Generate Certificate Request for Agent

The agent on Ribbon Application Management Platform (RAMP) requires an SSL certificate for secure communication between RAMP and registered devices. SSL certificates are issued by a Certificate Authority (CA). To issue certificates, a RAMP administrator must send a certificate service request (CSR) to a CA.

This section covers generating a CSR.

Start

1. Access RAMP as the insight user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the insight user.
2. Create the configuration file:

```
/opt/sonus/sonusComm/conf/cert/bin/manageCert config-csr
```

The configuration file `request-cert.cfg` is generated.

3. Edit the file `request-cert.cfg`. No commas are allowed for the key values.

Parameter	Description	Example	Mandatory (M)/ Optional (O)
cert.FQDN	The Fully Qualified Domain Name (FQDN) of the RAMP site. For example, if you plan to access your RAMP site from a browser using https://emshost.yourdomain.com, enter the FQDN value as "emshost.yourdomain.com". The FQDN must contain only alphanumeric characters, hyphens, and periods. Ensure that you have created a DNS entry for the FQDN to resolve it correctly to the RAMP IP address.	emsha1.sonusnet.com	M
cert.IP	The IP address of RAMP . Do not enter any value for the cert.IP parameter if you have generated the certificate service request (CSR) without an IP address.	10.155.75.200	M
cert.CN	The Common Name (CN) for the hostname.	ribbon.com	O
cert.organizationUnit	The department or division in the organization.	Purchasing	O
cert.organizationName	The name of the organization.	Ribbon Communications	O
cert.localityName	The name of the locality.	Westford	O
cert.stateName	The name of the state or province.	Massachusetts	O
cert.country	The two-letter country code.	US	O

4. Save the file.

5. Generate the CSR. The validity of a certificate is set to 1 year (365 days) by default. Change the certificate validity (in days) using the `-v` argument. The following is an example for generating a certificate service request with 30 days validity:

```
/opt/sonus/sonusComm/conf/cert/bin/manageCert gen-csr -v 30
```

Sample output:

```
Creating a certificate request with following settings:
Fully Qualified Domain Name .. ....: treebeardVM3
Certificate validity period ....., 30 days
Do you want to proceed? [y|n]:
```

6. Enter "y". The request file is generated at `/opt/sonus/sonusComm/conf/cert/conf/treebeardVM3_SonusAgent.csr`.
7. Verify the certificate service request before sending it to the CA:

```
/opt/sonus/sonusComm/conf/cert/bin/manageCert verify-csr
```

- a. Check the hostname:

```
hostname
```

- b. (Optional) Remove ^M characters in the CSR:

```
dos2unix /opt/sonus/sonusComm/conf/cert/conf/<hostname>_SonusAgent.csr
```

- c. Check the contents in the CSR:

```
cat /opt/sonus/sonusComm/conf/cert/conf/<hostname>_SonusAgent.csr
```

8. Share the CSR with a CA to obtain certificates. To share the CSR with the CA, refer to [Import Certificates for Agent](#).

Import Certificates for Agent

This section covers importing certificates obtained from a Certificate Authority (CA) to the Ribbon Application Management Platform (RAMP). You will usually receive two or three certificate files (root, intermediate, and site). The 'site' certificate is for the RAMP host. The site certificate can have a dependency on an 'intermediate' certificate or 'root' certificate, or both. The intermediate certificate is optional.

RAMP certificates in X.509 format may have different extensions (.cer, .crt, .pem, .der, and so on). The certificates will work if they are in PEM (ascii) or DER (binary) format, irrespective of the file extension.

Prerequisites

- A [Certificate Request](#) for RAMP Agent is generated.

Start

1. Copy the certificates to the RAMP host, in the directory `/tmp`.
2. Access RAMP as the `root` user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as the `root` user.
3. Add permissions for the insight user to access the certificate files:

```
chown insight:insight /tmp/agent-site.cer
chown insight:insight /tmp/verisign-root-ca.cer
chown insight:insight /tmp/verisign-intermediate-ca.cer
```

4. Change to insight user:

```
sudo su - insight
```

5. Verify the certificates are available in RAMP:

```
ls -ltr /tmp/*.cer
```

Example output of three files containing certificates:

```
-rw-r--r--. 1 insight insight 1854 Jan 11 19:49 /tmp/agent-site.cer
-rw-r--r--. 1 insight insight 1964 Jan 11 19:50 /tmp/verisign-intermediate-ca.cer
-rw-r--r--. 1 insight insight 1566 Jan 11 19:50 /tmp/verisign-root-ca.cer
```

6. Add the paths for the certificates into the `conf/import-cert.cfg` config file, starting with the root certificate. You can keep any alias (key) for the root and intermediate certificates in the config file, but the alias has to be 'agent' for the site certificate (reply for the certificate request sent to CA earlier). If the root and intermediate certificates have been imported, they do not need to be specified again in the config file. The site certificate (with the 'agent' alias name) is required.

```
grep -v "#" /opt/sonus/sonusComm/conf/cert/conf/import-cert.cfg | grep =
verisign-root-ca=/tmp/verisign-root-ca.cer
verisign-intermediate-ca=/tmp/verisign-intermediate-ca.cer
agent=/tmp/agent-site.cer
```

7. If the certificates from the CA are obtained in a bundle format, for example as a PKCS 12 (`.pfx` file) or PKCS 7 (`.p7b` file), manually split the file into individual PEM-encoded certificate files, and then add the paths of those files in the `import-cert.cfg` file. For example, if you receive a `.p7b` file, you can convert it into a PEM-encoded file as follows (change input and output file names appropriately):

```
$ openssl pkcs7 -print_certs -in /tmp/incerts.p7b -out /tmp/outcerts.cer
```

8. Open the output file and place each `BEGIN CERTIFICATE` and `END CERTIFICATE` block (including those two lines), and place them in separate files.
9. Place the paths for these separate files into the `import-cert.cfg` file.
10. Verify the certificates before importing it to the Agent keystore. It is recommended that you verify the certificate fingerprints with the fingerprints provided by the CA. You can also specify the alias name using the `-n` argument to view the certificate for only that alias name, as specified in the `import-cert.cfg`

configuration file. If no arguments are provided, all the certificates mentioned in the configuration file are displayed.

For example, enter the following command to verify the certificate details for only the `agent` alias (site certificate):

```
/opt/sonus/sonusComm/conf/cert/bin/manageCert verify-cert -n agent
```

11. Perform one of the following, to import :
12. Stop the RAMP. Refer to [How to Start and Stop RAMP](#).
13. Import the certificate:

```
/opt/sonus/sonusComm/conf/cert/bin/manageCert import-cert
```

Example output:

```
Starting certificate imports
Validating certificate config
Importing following certificates:
  1. verisign-root-ca [file: /tmp/verisign-root-ca.cer]
  2. verisign-intermediate-ca [file: /tmp/verisign-intermediate-ca.cer]
  3. insight [file: /tmp/agent-site.cer]
Do you want to proceed? [y|n]:
```

14. Enter "y". The certificates are imported.
15. Start the RAMP. Refer to [How to Start and Stop RAMP](#).
16. Check whether certificates are installed on the RAMP:

```
/opt/sonus/sonusComm/conf/cert/bin/manageCert show-cert -n <alias name>
```

Example output of viewing the installed 'agent' (site) certificate

```
/opt/sonus/sonusComm/conf/cert/bin/manageCert show-cert -n agent
```

Communication between the RAMP and registered devices is secured.

Add an Intermediate Certificate in SSL Handshake

If an intermediate certificate on the Ribbon Application Management Platform (RAMP) is expired, perform the following procedure to add an intermediate certificate in the SSL handshake:

Start

1. Access RAMP as an `insight` user. Refer to [Log onto the RAMP CLI](#) for accessing RAMP as an `insight` user.
2. Stop the RAMP. Refer to [How to Start and Stop RAMP](#).
3. Import the certificate:

```
/opt/sonus/sonusComm/conf/cert/bin/manageCert import-cert
```

4. Enter "y". The certificates are imported.
5. Copy the intermediate certificate (or certificate bundle) to the directory `/etc/httpd/conf/`.
6. Edit the file `/opt/sonus/ems/weblogic/sonusEms/data/sys/emsapps_apacheproxy_virtual_host.conf`.
7. Uncomment the following line and update it with the correct name for the intermediate certificate (or certificate bundle):

```
SSLCertificateChainFile /etc/httpd/conf/<Name of Intermediate Cert>
```

Example output:

```
SSLCertificateChainFile /etc/httpd/conf/DigiCertCA.crt
```

8. Start the RAMP. Refer to [How to Start and Stop RAMP](#).

Renew RAMP Certificates

In this section:

- [Generate certificates](#)
- [Regenerate the Default Self-Signed RAMP GUI Certificates](#)
- [Regenerate DBaaS Certificates](#)
- [Generate Certificates for Upgraded Versions of pre 24.12 RAMP](#)
 - [Cloud Upgrade](#)
 - [KVM/VMWare Backup and Restore](#)
 - [Generate Certificates for RAMP 24.12 and Forward](#)

To renew certificates expiring on the Ribbon Application Management Platform (RAMP), generate new certificates for existing RAMP versions below RAMP 24.12. Renew the certificates using the scripts `generateCerts.sh` and `updateRDCerts.sh`. These scripts are available in the `rampbootstrap.tar` file.

You are allowed to run only the `generateCerts.sh` script. If the RAMP is in a geographically redundant (GR) setup, the `updateRDCerts.sh` is run automatically within the file `generateCerts.sh`.

These scripts support both Standalone and GR scenarios.

Prerequisite

All services are deployed before triggering the `generateCerts.sh` and `updateRDCerts.sh` scripts.

Generate certificates

Use the following procedure to generate a new certificate:

Start

1. Log on to the RAMP as an `admin` user.
2. Download the `rampbootstrap.tar` file from the Ribbon Support Portal.
3. Copy the downloaded files from the `generateCertificate` folder to the RAMP `/home/admin/` directory:

```
cp /home/admin/
```

4. Change permissions of both the files:

```
chmod 740 generateCerts.sh  
chmod 740 updateRDCerts.sh
```

5. For a GR setup:

Note

This step is applicable only for a GR RAMP.

- a. Log on to the active or standby RAMP as an `admin` user.
- b. Navigate to the folder where the files are extracted and copy the files to the directory `/home/admin/`:

```
scp generateCerts.sh updateRDCerts.sh admin@<target-ip>:/home/admin/
```

For a RAMP GR, the system does not prompt for a password.

6. Stop the RAMP. Refer to [How to Start and Stop RAMP](#).

Note

For a RAMP GR, perform this command on either the active or standby.

7. Run the script `generateCerts.sh`. Provide the function name to generate the certificates for a specific purpose:
 - a. Change to `root` user:

```
sudo su -
```

- b. Run the `generateCerts.sh` command:

```
[root@rakeshramp: /home/admin ]#./generateCerts.sh
```

Example output:

```
[2024-11-07 12:11:08 root@rakeshramp: /home/admin ]#./generateCerts.sh
Usage: ./generateCerts.sh <function_name>
function_name :-
    generateDemoCert - Generate Demo Insight Certificate

    generatenewCertsall - Generate All Certificates MS and Insight

    DistributeCert - Distribute keys to Target , need UpdateRDCerts file to run
    this on both servers

    copycerts - copy certificates to RAID
    dm_gen_cert - DEVGMT certificate Generation
    pm_gen_cert - PM certificate Generation
    lm_gen_cert - LM certificate Generation
    aa_gen_cert - AA certificate Generation
    generate_acs_certificate - AS certificate Generation
    generate_oss_certificate - OSS certificate Generation
    generate_gss_certificate - GSS certificate Generation
    generate_nms_certificate - NMS certificate Generation
    generate_ev_certificate - EV certificate Generation
```

Regenerate the Default Self-Signed RAMP GUI Certificates

This procedure regenerates the default self-signed RAMP GUI certificates. For the RAMP GR, perform this procedure on both, the active and standby RAMPs.

Start

1. Log on to the RAMP as an `admin` user.
2. Download the `rampbootstrap.tar` file from the Ribbon Support Portal.
3. Copy the downloaded files from the `generateCertificate` folder to the RAMP `/home/admin/` directory:

```
cp /home/admin/
```

4. Change the permissions of both the files:

```
chmod 740 generateCerts.sh
chmod 740 updateRDCerts.sh
```

5. For a GR setup:

Note

This step is applicable only for a GR RAMP.

- a. Log on to the active or standby RAMP as an `admin` user.
- b. Navigate to the folder where the files are extracted and perform the following:

```
scp generateCerts.sh updateRDCerts.sh admin@<target-ip>:/home/admin/
```

Since it is a RAMP GR, the system should not ask for a password.

6. Stop the RAMP. Refer to [How to Start and Stop RAMP](#).
7. Run the `./generateCerts.sh generateDemoCert` script on the RAMP. If it is a GR setup, run this script on the active and standby RAMPs:

```
[root@rakeshramp: /home/admin ]# ./generateCerts.sh generateDemoCert
```

8. Start the RAMP. Refer to [How to Start and Stop RAMP](#).

The self-signed GUI certificate is updated.

Regenerate DBaaS Certificates

Use this procedure only when you want to generate the DBaaS certificates.

Reusing Cinder on the new RAMP with a change in the IP address results in reuse of the certificates in the folder `/opt/raid/CA/` from the older RAMP that was deleted. The certificates have the SAN IP address and the Hostname of the old RAMP.

To update the certificates with the latest SAN IP address, run the command `generateCerts.sh` with the option `generatenewCertsall`.

Start

1. Log on to the RAMP as `admin` user.
2. Download the `rampbootstrap.tar` file from the Ribbon Support Portal.
3. Copy the downloaded files from the `generateCertificate` folder to the RAMP `/home/admin/` directory:

```
cp /home/admin/
```

4. Change permissions of both the files:

```
chmod 740 generateCerts.sh  
chmod 740 updateRDCerts.sh
```

5. For a GR RAMP setup:

Note

This step is applicable only for a GR RAMP.

- a. Log on to the active RAMP as an `admin` user.
- b. Copy the files to the standby RAMP, if the files already exist, then both the files should be in the same path as the active RAMP path:

```
scp generateCerts.sh updateRDCerts.sh admin@<target-ip>:/home/admin/
```

Since it is a RAMP GR, the system should not ask for a password.

6. Stop the RAMP. Refer to [How to Start and Stop RAMP](#).

For a RAMP GR, perform this command on either the active or standby.

7. To regenerate the certificates:

```
[root@sanrampperf1-rampcnf-0: /home/admin ]# ./generateCerts.sh  
generatenewCertsall
```

You do not have to run this command on the standby RAMP.

8. Start the RAMP. Refer to [How to Start and Stop RAMP](#).

On completion of this procedure:

- All the services are running with the latest certificates.
- The system backs up the Insight Certificates in the `/opt/raid/CA` folder. These certificates are used during an upgrade.

Generate Certificates for Upgraded Versions of pre 24.12 RAMP

If you regenerated the certificates for the RAMP based on the above procedures for the RAMP GUI and DBaaS certificates, then RAMP retains these regenerated certificates when you upgrade the RAMP to any version less than the RAMP 24.12.

Cloud Upgrade

Certificates are generated when you upgrade, for the RAMP versions less than 24.12 and if you did not regenerate the certificates performing the above procedures for the RAMP GUI and DBaaS Certificates.

To upgrade, refer to [Upgrading RAMP](#).

KVM/VMWare Backup and Restore

If certificates are regenerated before taking a backup of the RAMP, when restoring the backup it uses the existing certificates. If not, it generates new certificates at the end of restore.

Prerequisites

Perform the procedures in sections:

- Regenerate the Default Self Signed RAMP GUI Certificate and
- Regenerate DBaaS Certificates

To backup and restore the RAMP, refer to [Backup and Restore](#).

Generate Certificates for RAMP 24.12 and Forward

Certificates are generated when you install the RAMP.

You need not regenerate the certificates. To regenerate certificates while troubleshooting, perform the following procedure:

Reusing Cinder on the new RAMP with a change in the IP address results in reuse of the certificates in folder `/opt/raid/CA/` from the older RAMP that was deleted. The deleted files have the SAN IP address and the Hostname of the old RAMP.

To update the certificates with the latest SAN IP address, run the command `generateCerts.sh` with the option `generatenewCertsall`.

Start

1. Log on to the RAMP as an `admin` user.
2. Change to root user:

```
sudo su -
```

3. Stop the RAMP. Refer to [How to Start and Stop RAMP](#).

For a RAMP GR, perform this command on either the active or standby.

4. Navigate to the folder `/opt/sonus/ems/conf/`

```
cd /opt/sonus/ems/conf/
```

5. Run the script: `generateCerts.sh` with the function `generatenewCertsall` to generate certificates for RAMP and all the microservices (Regenerate DBaaS certificates):

```
[root@rakeshramp: opt/sonus/ems/conf]# ./generateCerts.sh generatenewCertsall
```

6. Regenerate the certificates using:

```
[root@rakeshramp: opt/sonus/ems/conf]# ./generateCerts.sh generateDemoCert
```

Enable Key-Based Authentication for SSH

Use this procedure to enable key-based authentication for SSH on a host machine.

After completing this procedure, you can log into a target machine using a target user account from a host machine, without any password. The following is the explanation of the terms used in the procedure:

- Host Machine: This machine is used to log onto the target machine.
- Host User: The user on the host machine used to log into the host machine.
- Target Machine: The machine to which you want to log onto from another machine.
- Target User: The user account on the target machine to use to log onto the target machine.

Start

1. Log onto the host user account on the host machine using SSH.
2. Change to the host user's ssh directory:

```
$ cd .ssh
```

3. Check if `id_rsa` and `id_rsa.pub` exists by executing the following command:

```
$ ls
```

If `id_rsa` and `id_rsa.pub` files exist, go to step 6.

4. Execute `ssh-keygen` to generate the public or private RSA key pair:

```
$ ssh-keygen -t rsa
```

5. Press **ENTER** to save the key files or passphrase.

The `ssh-keygen` utility generates a private key file as `id_rsa` and a public key file as `id_rsa.pub`.

6. Copy the `id_rsa.pub` file to `<hostname>.pub` file:

```
$ cp id_rsa.pub <hostname>.pub
```

For example, if the hostname is `jupiter`, then enter the following:

```
$ cp id_rsa.pub jupiter.pub
```

7. Copy the public key file `<hostname>.pub` to the target user's `.ssh` directory on the target machine:

```
$ scp <hostname>.pub <targetuser>@<targetmachine>:~/.ssh/<hostname>.pub
```

For example, if the hostname is `jupiter`, `targetuser` is `admin`, and `targetmachine` is `nmhost`, then enter the following:

```
$ scp jupiter.pub admin@nmhost:~/.ssh/jupiter.pub
```

8. Log into the target user's account on the target machine using SSH:

```
$ ssh <targetuser>@<targetmachine>
```

For example, if `targetuser` is `admin` and `targetmachine` is `nmhost`, then enter the following:

```
$ ssh admin@nmhost
```

9. Change to the target user's `.ssh` directory:

```
$ cd .ssh
```

10. Append the contents of the host user public key file to the file `authorized_keys`:

```
$ cat <hostname>.pub >> authorized_keys
```

For example, if the hostname is jupiter, then enter the following:

```
$ cat jupiter.pub >> authorized_keys
```

11. Change the permissions on the file `authorized_keys`:

```
$ chmod 644 authorized_keys
```

12. Exit the target machine and log into the target machine again from the host machine:

```
$ ssh <targetuser>@<targetmachine>
```

For example, if targetuser is admin and targetmachine is nmhost, then enter the following:

```
$ ssh admin@nmhost
```

Obtain the RAMP SSH Keys

Use the following procedure to obtain the SSH keys for Ribbon Application Management Platform (RAMP) after the instance is up and running. If your network includes a Ribbon PSX that will be managed by RAMP, the PSX uses the RAMP key when it is instantiated. In case of a disaster, you need the SSH keys to restore a RAMP instance.

After obtaining the SSH keys, copy the key information to an external server.

Complete the following steps to obtain the SSH key information from RAMP:

1. SSH to the RAMP IP address, for example:

```
ssh insight@10.14.55.120
```

2. Execute the following command:

```
cd .ssh
```

3. Execute the following command:

```
ls -l
```

The following is a sample output:

```
-rw-----. 1 insight insight 397 May 22 18:48 authorized_keys
-rw-----. 1 insight insight 1679 May 22 18:12 id_rsa
-rw-r-----. 1 insight insight 394 May 22 18:12 id_rsa.pub
-rw-r--r--. 1 insight insight 32644 May 25 17:36 known_hosts
```

4. Enter the following command to obtain the public SSH key:

```
cat id_rsa.pub
```

The SSH key is displayed, for example:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCYpnuLMLZLJxgxvgkUdiy3SW5xL4uLLcpAQy2P6fdyrThWL0PiPH
8R0JjXn6PeYvcj69Qis0Hgb736RpoapaLpYcsA1qcHL07503174ImNsjr3c8b9uza50Bt5dXgo4ChBZjW
9cKa4DCyqiemeFvg3bot7q1LoVi/
cS43VFv+EPLL8fxQAZ2p8+6B2c0fsgREGTeAS111i9b2i456uC+fWvgiimMk8Zuzg9kCqkhneb7LHPmR/
KiDlhv5krXE0+P3g6co/01Mxi1bx7/8bprbTq6m71uOP4e6H+F9/fD++BmP/
dk7x1uB289Y6ZHtFXjdHRHLpk1CFmw7toyZ0Swj
insight@keep-freis-ems-a310
```

Note

When instantiating a PSX primary in OpenStack, there is a parameter called EMS Public Ssh Key. Use the key you retrieved with that parameter to enable RAMP to access the PSX without a password.

5. Enter the following command to obtain the private ssh key:

```
cat /opt/sonus/ems/.ssh/id_rsa
```

The SSH key is displayed, for example:

```
-----BEGIN RSA PRIVATE KEY-----
MIIIEowIBAAKCAQEA3szwWsndur3T72jJIDoKiMaIk0kuKdKMqADc0jtFvE8GWdYz
X2RS5qF1nLzfj4ui0cx/Cx/+EZMrJrnf/GH4nH6DRJaUtQglFo62NgPNZGgONADj
ThGLABjKLU07iDV5XeFPrZxzUSd72uPSEXK5w6f1uo9q06UbbAgSdPwnnk1ChKcS
GcbE7fNGe/wEtKYmsRw8ALe6FIzu9WRA0dbApLzLSZC5kV+PE7rC0f0qZiNjheZV
/lzbu0T3quAJD6reuSzEAzWJ9HhSLQa50X0GD+vyzRpAQnHi4EERZWV6zGNdhTaI
rUyRqjMzFMmDYnwE4aDJFs2RAYnwWTtYW4hH6QIDAQABAOIBACT3rESZCGtQcbK5
rN0ev0NkDhUxiRIbw9lbIZwyyC4u9LvurX3qrzYL0xQLkWhJojr7rVK7pSbM8YA
aZShwJE3LYCiKC0Rg7rc60us3juCmZLHwZEPnDNior8n3D98v0rzlEn4xf7FR0Kz
Q96nlVp4wFY/eKheU/VFteQg9dHJungGKmCw3tizBqXo7LIuP9paTDcWTWdta0Yf
rWVpY0968yrjx3PdJF06DHGgK9XeJ0CoRKMMzS8x0jhnWy/7ruRayZtXvLdYT0Iu
nWcNFvgW0qFSz0ADCUmj51Pa47dLsAdyY1VjN8Ou3ZczNnPKizz9P7gP52jpw0dk
XrIL8AECgYEA+Rd6+USKEiKSUD+t00/jTcm0PYdBrEX3+raJawTa08u6NHE3QJnn
g0NvaLLIeNAihQuW6KLSKx1gCIFWJk278irwjiSp97+vMCGhXyp1s5eIROX60RjV
LWPjm49loJkVyqUs6LWkSmFrRGB1SPuTSKaVayQNCTfFRt6mVnaE8wECgYEA5PrL
Yhh21u/tqzb9iIAZgFrjt885f3ToUZjSXKEvflUqa3sbzFhSrnrEJAd80sgM2n2m
Yn5bUmJvzYVeFgbfDJeIIuLNj+brhSYdKdh5zB6nx4cmJm0zSaJiAYN2/cFuLtKx
1U9sHA8a9Zip+j+0vqSC+C1NvETtgqleJUjzH0KcGYBm2V8ZVVI5fWPmZqRsFQvp
roMRdKuVKj698mjCb7Y7BT+ZL7YUoneJJ2r02/0ShT38QnDzYCEdnD9uw5iCsE40
K9SvnEvH0+/N+9TZqnp28PZ/HEZ3170NNTSA19/9DWf0pxUacuWOpFD5mAHA9Ty
znVwmo4XZE08g2pDASTCAQKBgF8X7HkLsebnC2ukhbw3ft+4X1PJopZVJdolPk+r
vP3sevZyBQRjNcsvi9Durx8WZ4ghoITM9v4K1Wwj2oQJTH5909NjH5eAjhUY1Am5
1jM4E/OgI+7XcPJG1q8M0tF9kFwvuJzexAYPG+IdCZJc7NotlhqdLehfM8gMsIWJ
ezVpAoGBAKRx84JkNDNJ9SZtFSNxxDMzd/uRKbk9wntBF0sBNCrtqNsx/OCsZHye
```

```
CQ75MSxDL5NSOWtCK2Ln9fqAid/3rNsbwhFtMDKEEXn0oLLiN6wy9o/N8312VW4o
f/NTRELwvBssAovC7SWiTtap67H5Mi/H9t8z/bFEPW6ptBYaxsQH
-----END RSA PRIVATE KEY-----
```

6. Perform any of the following:
 - Copy the output from steps 4 and 5 to a text file, and copy to an external server.
 - Transfer the `id_rsa` and `id_rsa.pub` files to an external server.
7. Copy `authorized_keys` to an external server.
8. Copy `known_hosts` to an external server.

Manually Generate Traps and Verify Alarm Handling

In this section:

- [Parse MIB to JSON/HTML](#)
 - [Examples to parse MIB to JSON](#)
- [Generate Traps](#)
- [Configure SNMPv3 Receiver Using snmptrapd to Test SNMPv3 Traps](#)

The Ribbon Application Management Platform (RAMP) supports the `genTraps.sh` script. As a `root` user, you can use this script to send alarms and events manually to pre-configured IP addresses (IPv4, IPv6, and FQDN) and ports. This script is in `/opt/fm/bin/random-trap-generator/genTraps.sh`.

Use the `genTraps.sh` script to generate all the SNMP traps based on a MIB file and verify that all the available alarms are handled appropriately.

Note

This feature is not REST exposed and is only available if invoked from the Linux shell. This feature does not support clearing of problem events/traps/notifications. Problem and Clearing events are treated as independent notifications. This feature does not support filtering/skipping deprecated alarms. Hence, any alarm marked as deprecated is generated unless filtered with the option of filtering traps.

Note

While using the `genTraps.sh` script, you may encounter certain errors and warnings, although traps are generated successfully. Ribbon assures you that these occurrences, though noted, do not necessarily indicate a failure to complete the task. Ribbon's tool is designed to manage various scenarios gracefully, ensuring successful process completion.

Ribbon advises you to proceed confidently and avoid being deterred by transient error messages. Further investigation is needed only if the command does not work as expected to address any underlying issues. Such logs are then helpful in proceeding with the investigation.

The `genTraps.sh` script may generate error messages such as:

Example Error Message:

```

Textual convention doesn't map to real type (Unsigned64): At line 38 in /opt/fm/
metadata/mib/import/SMIv2/SNMPv2-SMI
: (is a reserved word): At line 38 in /opt/fm/metadata/mib/import/SMIv2/SNMPv2-SMI
18446744073709551615 (is a reserved word): At line 38 in /opt/fm/metadata/mib/import/
SMIv2/SNMPv2-SMI
Bad operator (:): At line 16 in /opt/fm/metadata/mib/import/SMIv2/RMON-MIB
Did not find 'EntryStatus' in module RFC1271-MIB (/opt/fm/metadata/mib/import/SMIv2/
TOKEN-RING-RMON-MIB)
Did not find 'OwnerString' in module RFC1271-MIB (/opt/fm/metadata/mib/import/SMIv2/
TOKEN-RING-RMON-MIB)
Unlinked OID in TOKEN-RING-RMON-MIB: tokenRingPHistoryTable ::= { history 4 }
Undefined identifier: history near line 951 of /opt/fm/metadata/mib/import/SMIv2/TOKEN-
RING-RMON-MIB
Should be STATUS (DESCRIPTION): At line 44 in /opt/fm/metadata/mib/import/SMIv2/FOUNDRY-
SN-SW-L4-SWITCH-GROUP-MIB
Bad parse of OBJECT-TYPE: At line 44 in /opt/fm/metadata/mib/import/SMIv2/FOUNDRY-SN-SW-
L4-SWITCH-GROUP-MIB
Cannot adopt OID in xxxx-MIB: etherStats2Entry ::= { etherStats2Table 1 }
Cannot adopt OID in xxxx-MIB: hostControl2Entry ::= { hostControl2Table 1 }

```

Prerequisites

- mib2c - MIB parser. This is part of the net-snmp-perl Linux package.
- To configure an SNMPv3 trap receiver, use the `engineId` as 80001370010a360d50b0aabc25, which is required for the trap sender to send it to the receiver.

Parse MIB to JSON/HTML

Parse the MIB and generate the JSON file:

```
genTraps.sh -d <MIB-DIR-PATH> -m <MIB-MODULE-NAME> [-k] [-o <JSON OUTPUT DIR>] [-j <JSON FILE PATH>]
```

Parameters

Parameter	Length/Range	Description	Mandatory/Optional
Name	1 to 64 characters. Do not use special characters like <code>^[^<>.:,;+=*?\"<> !@#\$\$%^&() `{}]*\$</code>	Name of the MIB module. The default name is <code>sonusEmsMib</code> . The <code>sonusEmsMib</code> is the base module containing all the RAMP traps defined in the MIB files in the MIB directory.	M

Parameter	Length/Range	Description	Mandatory/Optional
Directory Path		Path to the directory where all the MIBs are stored. The default path is located in the RAMP alarms MIB <code>/opt/fm/metadata/mib/import/SMIv2</code>	M
Output Directory		The output directory where the <code>.JSON</code> file is generated. The default directory is <code>/tmp/</code> .	M
-h		Provides the list of parameters and options used along with the command.	NA
Parser Parameters			
-d		Specify the directory containing MIBs and its dependencies.	M
-m		Specify the MIB Module Name.	M
SNMP Parameters			
-i		The trap receiver address [IPv4 / IPv6 / FQDN].	M
-p		The trap receiver port.	M
-u		USM Username.	M
-w		SNMPv3 AuthNoPriv. Specify Authentication Protocol MD5/SHA.	M
-x		SNMPv3 AuthNoPriv. Specify Authentication PassPhrase	M
-y		SNMPv3 AuthPriv. Specify Privacy Protocol [AES/DES/DES3]	M
-z		SNMPv3 AuthPriv. Specify Privacy PassPhrase	M
Optional Parameters			

Parameter	Length/Range	Description	Mandatory/Optional
-v	1 - 3	The SNMP version. v1/v2c/v3. The default value is 2.	O
-n		The trap interval in nanoseconds. The default is 200000ns resulting trap-rate = 500tps.	O
-j		The .JSON file to generate the notifications contained in it.	O
-f		The text file contains the event/alarm name list to filter during trap generation.	O
-o		The output directory for .JSON/HTML file generation. The default value is /tmp .	O
-k		Parse the MIB and generate documentation in HTML format.	O
-q		For random trap generation. Specify in seconds how long trap generation will run. The default value is 0.	O

Examples to parse MIB to JSON

In this scenario, `sonusConnexIpTrapsMIB` is an example MIB file.

Perform the following procedure to generate traps from `sonusConnexIpTrapsMIB` :

1. Create the directory `sbcMIBs` :

```
mkdir /opt/sbcMIBs/
```

2. To generate traps using `genTraps.sh`, ensure all the required MIB files are available in one directory. In this case, `sonusConnexIpTrapsMIB` relies on the MIBs found in `/opt/fm/metadata/mib/SBX5K/SMIv2/` and `/opt/fm/metadata/mib/import/SMIv2/`. Copy all the MIB files from these two directories into `/opt/sbcMIBs/` to generate traps from `sonusConnexIpTrapsMIB`.
 - a. Copy the MIB files from `/opt/fm/metadata/mib/SBX5K/SMIv2/`


```
cp -r /opt/fm/metadata/mib/SBX5K/SMiv2/* /opt/sbcmibs/
```

- b. Copy the MIB files from `/opt/fm/metadata/mib/import/SMiv2/`

```
cp -r /opt/fm/metadata/mib/import/SMiv2/* /opt/sbcmibs/
```

3. Change the directory to `random-trap-generator` :

```
cd /opt/fm/bin/random-trap-generator
```

4. Parse only the alarms:

```
./genTraps.sh -d /opt/sbcmibs/ -m sonusConnexIpTrapsMIB -i <ramp-ip> -p <port>
```

Example input:

```
./genTraps.sh -d /opt/sbcmibs/ -m sonusConnexIpTrapsMIB -i 10.52.161.96 -p 162
```

Example output:

```
[2024-07-11 22:16:42 root@sanramp-rampcnf-0: /opt/fm/bin/random-trap-
generator ]# ./genTraps.sh -d /opt/sbcmibs/ -m sonusConnexIpTrapsMIB -i 10.52.161.
96 -p 162
-----DEFAULTS / INPUTS-----
MIB2C PATH = /bin/mib2c
Translate MIB to JSON = Yes
MIB2c Config = /opt/fm/conf/random-trap-generator/mib2json.conf
MIB Location = /opt/sbcmibs/
MIB Module Name = sonusConnexIpTrapsMIB
JSON Location = /tmp/
Generate Alarms = Yes
IP = 10.52.161.96
PORT = 162
SNMP Version = 2
TRAP Interval (Nanoseconds) = 20000000
TRAP Filter File = 0
Trap Generation = Sequential
-----

Successfully generated JSON : /tmp/sonusConnexIpTrapsMIB.json
Total Events in MIB : 20
Filter Applied : false
```

```

Trap Generation : Non-timed Trap Generation
Starts sending alarms... 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13,
14, 15, 16, 17, 18, 19, 20, Done
Total traps triggered: 20
Time elapsed: 0.40 seconds
Rate: 50.13/sec

[2024-07-11 22:16:46 root@sanramp-rampcnf-0: /opt/fm/bin/random-trap-generator ]#

```

Parse and send RAMP alarms:

```
./genTraps.sh -i 127.0.0.1 -p 162
```

Parse only the alarms:

```
./genTraps.sh -d /opt/sbcmibs/ -m sonusConnexIpTrapsMIB -o /opt/
```

Parse and send SNMPv2:

```
./genTraps.sh -d /opt/sbcmibs/ -m sonusConnexIpTrapsMIB -i 10.85.56.35 -p 2300
```

Parse, filter, and send SNMPv2:

```
/genTraps.sh -d /opt/sbcmibs/ -m sonusConnexIpTrapsMIB -i 10.54.28.96 -p 162 -f /opt/
trapList.txt
```

Parse and send SNMPv3:

```
./genTraps.sh -d /opt/sbcmibs/ -m sonusConnexIpTrapsMIB -i 10.54.5.53 -p 162 -v 3 -u
ribbon -w SHA -x sonus123 -y DES -z sonus123
```

Parse MIB to HTML:

In this example the MIB is stored in `/opt/fm/metadata/mib/import/SMIv2`

```
genTraps.sh -d /opt/fm/metadata/mib/import/SMIv2/ -m sonusEmsMIB -k
```

Generate Traps

To generate the traps:

```
genTraps.sh [-k] [-o <JSON OUTPUT DIR>] [-j <JSON FILE PATH>] [-f <TrapList File>] [-n
TrapInterval] [-q <TimeToRun>] -i <IP> -p <Port> [-v <SNMPVersion>] [[-u<Username> -w
<AuthProtocol> -x <AuthPassPhrase> [-y <PrivacyProtocol> -z <PrivacyPassPhrase>]]
```

Parameters to generate traps

Parameter	Description	Range/Length
Username	Provide a unique user name.	1 to 64 characters. Do not use special characters like <code>^[^<>.:,+=*?\"<> !@#\$\$%^&() `{}]*\$</code>
USM Security Name	Provide the security name needed for SNMPv3.	5 to 32 alphanumeric characters.
Authentication Protocol	Specify the authentication protocol. Select Message Digest (MD5) or Secure Hash Algorithm (SHA) as the protocol to enable private interactions over secure channels. - MD5 - SHA The default value is "SHA".	NA
Authentication Passphrase	This is the SNMPv3 authorization password. The default value is "admin123".	8 to 32 characters.
Privacy Protocol	Select Data Encryption Standard (DES) or Advanced Encryption Standard (AES) authentication protocol. - AES - DES The default value is "AES".	
Privacy Passphrase	This is the SNMPv3 privacy password. The default value is "admin123".	8 to 32 characters.
Destination IPv4 / IPv6 address / FQDN	Provide the trap receiver's address. - IPv4 address - IPv6 address - FQDN	
Destination Port	Provide the destination port number. The default value is "162".	

For example, `trapListFile.txt` contains four event names that are filtered from the `.JSON` file and sent to the receiver:

Example:

```
trapListFile.txt---
sonusEmsPMExportSFTPFailClearNotification
sonusEmsPMExportSFTPFailNotification
ribbonNodeCeasedOpsNotification
ribbonEVServiceZTPConnectivityLostNotification
```

Configure SNMPv3 Receiver Using snmptrapd to Test SNMPv3 Traps

To generate and test the SNMPv3 alarms, configure the SNMPv3 receiver using the same `engineID` that is received from the sender.

Start

1. Log on to RAMP as `root`.
2. Create a file `/tmp/snmptrapd.conf`
 - a. Use `80001370010a360d50b0aabc25` for engine Id:

```
createUser -e 0x<SENDER_ENGINE_ID> <Username> <AuthProtocol> <AuthPassPhrase>
<PrivProtocol> <PrivPassphrase>
```

- b. `authuser log <Username>`
3. Identify the process running on the default port 162 and stop the process.
 - a. Identify the process:

Example:

```
[2023-07-27 21:39:19 root@cmpsource: /home/admin ]# lsof -i:162
```

Example Output:

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE/OFF	NODE	NAME
java	13153	insight	14u	IPv6	88472	0t0	UDP	*:snmptrap

- b. Stop the process:
- ```
kill -9 13153
```
4. Start the `snmptrapd`. This runs in the foreground, uses only the specified config file and logs the value in the `stderr`:

**Example:**

```
snmptrapd -f -C -c /tmp/snmptrapd.conf -Le
```

**Example Output:**

```
[2023-07-27 21:40:35 root@cmpsource: /home/admin]# snmptrapd -f -C -c
/tmp/snmptrapd.conf -Le
NET-SNMP version 5.8 AgentX subagent connected
NET-SNMP version 5.8
```

5. Use the `./genTraps.sh` to display the SNMPv3 alarms on the `snmptrapd` receiver console.

**Note**

snmptrapd may not support auth/priv protocols other than SHA/MD5 & AES/DES

## Proxy Manager

The proxy manager meets the Ribbon Application Management Platform (RAMP) security requirements. You can route all external RAMP connections through the HTTPS proxy server, which is exclusively used for external connections to services such as Ribbon Audit Portal (RAP), IDH/STI Server, ZTP Server, AWS billing uploads, and other similar services.

The RAMP provides a UI option to configure multiple proxy servers with each GR site with different proxy servers. The attributes of the proxy server configuration include:

- **Proxy Name** – A unique Proxy Name
- **Proxy Host IP** – Proxy IP Address
- **Proxy Port** – Proxy Port
- **Proxy Username** – Proxy Username
- **Proxy Password** – Proxy Password
- **HostName Matching Pattern** – A regex pattern used to help choose proxies to corresponding instances such as in a geo-redundant deployment.
- **Description** – Proxy Description (if any)

**Prerequisites:**

- The host and port parameters are essential to establish a proxy server and are unique with each configuration. The username and password parameters are optional to restrict access to the proxy.
- The `hostnameMatchingPattern` parameter is a regex pattern associating a proxy configuration with a specific hostname. This helps to assign proxies to corresponding instances in a geo-redundant deployment.

**Note**

The applications: LM, EV, and STI use the same proxy, and opt whether to use a proxy or not. An application-level configuration is provided to determine enable/disable the use of proxy. When the proxy is down, the RAP registration and the postpaid report upload fails.

The Primary RAMP interface connects the RAMP to the proxy, and the Secondary IP for device communication.

Perform the following procedure to forward the external RAMP connections through the HTTPS proxy server:

**Start**

You can have multiple proxy servers, but the RAMP follows only the hostname matching based pattern.

1. Log on to the RAMP GUI.
2. Navigate to **SYSTEM > Interfaces > Https proxy**.
3. To create a proxy, click **Add Proxy**.
4. Enter the details that includes **Proxy Name, Proxy Host IP, Proxy Port, Proxy Username, Proxy Password, HostName Matching Pattern, Description** and click **Save**. A message displays confirming the new HTTP Proxy is created.

To use the proxy in any application that supports communication through a proxy, go to the respective application and enable the option (the option is set to false by default). You can create, edit, or delete the proxy as you require. If you delete the proxy, the application loses internet connectivity.

5. If you desire to use a proxy, use the option **Use Proxy configured on the RAMP to connect to IT** in the **Administration** page.

For edge features like ZTP registration/AWS billing, navigate to **EdgeView Service Administration** and enable the **RAMP Internet Proxy** option.

## Legacy Device Management

The Ribbon Application Management Platform (RAMP) supports legacy device management when **Federal Information Processing Standards (FIPS)** are disabled.

You can configure OpenSSH to use older or weaker algorithms when dealing with legacy devices like GSX/DSI/SBC (that are not updated to support modern cryptographic standards).

Modern OpenSSH configurations typically disable these older algorithms by default for security reasons. This causes RAMP connectivity issues with devices offering weak ciphers.

The script `updateSystemCryptoPolicy.sh` is designed to manage cryptographic policies on a Linux system, focusing on ensuring the policy is set to default. If not, it provides options to restore the original policy. It also checks if the user is root and if FIPS mode is disabled, as these conditions impact the ability to change the cryptographic policies. The default policy allows the weaker algorithms while dealing with legacy devices such as GSX/DSI (that are not updated to support modern cryptographic standards).

You can access the script at `/opt/sonus/ems/conf/security`.

**Note**

For non-FIPS environments, this script allows RAMP to manage communication between legacy devices like GSX-DSI over SSH and other GSX functionalities that need SSH tunneling to DSI over weak ciphers.

When FIPS is enabled, no action is taken, and the script exits.

The new root owned script `/opt/sonus/ems/conf/security` updates the system-wide crypto policies.

Perform the following to execute `updateSystemCryptoPolicy.sh` script.

**Start**

1. Log on as a `root` user.

```
cd /opt/sonus/ems/conf/security
```

2. Verify the current crypto policy.

```
update-crypto-policies --show
```

**Example Output:**

```
DEFAULT:NO-SHA1:NO-CBC:NO-HMAC-SHA1
```

```
The RHEL8 system default policy is DEFAULT:NO-SHA1:NO-CBC:NO-HMAC-SHA1
```

3. Run the following, to change the policy to default to allow weaker algorithms.

```
./updateSystemCryptoPolicy.sh
```

**Example Output:**

```
Current crypto policy: DEFAULT:NO-SHA1:NO-CBC:NO-HMAC-SHA1
Backing up the current policy...
System-wide crypto policy is successfully set to DEFAULT
```

4. Verify the current policy.

```
update-crypto-policies --show
```

**Example Output:**

```
DEFAULT
```

5. Verify the SSH communication by discovering the GSX.

## Revert Procedure

This restores the original cryptographic policy from a backup file ( `/etc/crypto-policies/system-default-policy.txt` ).

1. Log on as a `root` user.

```
cd /opt/sonus/ems/conf/security
```

2. Run the following command as a `root` user, if the policy needs to be reverted to system default.

```
./updateSystemCryptoPolicy.sh -r
```

**Example Output:**

```
./updateSystemCryptoPolicy.sh -r
Reverting crypto policy to system default: DEFAULT:NO-SHA1:NO-CBC:NO-HMAC-SHA1
Crypto policy is successfully reverted to system default: DEFAULT:NO-SHA1:NO-
CBC:NO-HMAC-SHA1
```



### 3. Verify the policy.

```
update-crypto-policies --show
```

**Example Output:**

```
DEFAULT:NO-SHA1:NO-CBC:NO-HMAC-SHA1
```

# REST API Documentation

In this section:

- [Accessing the API Documentation from RAMP](#)
  - [View RAMP API User Documentation](#)
  - [Download RAMP API Definition Files](#)
- [Authentication Requirements](#)
  - [Obtain a Token Using a Username and Password](#)
  - [Obtain a Token using a SAML Service Provider](#)
  - [Refresh an Authentication Token](#)
- [Role-Based User Access Requirements](#)
- [Terminating a Session](#)

Related articles:

- [Example API Requests and Responses](#)

This document provides information and examples for using Ribbon Application Management Platform (RAMP) Representational State Transfer (REST) APIs.

Ribbon Application Management Platform (RAMP) provides Open API 3.0-compliant REST APIs as an alternative way to accomplish many of the tasks that users perform using the RAMP user interface (UI). This enables users to programmatically manage or script these tasks if they choose.

The RAMP APIs adhere to the simple, stateless architecture style defined by REST and they follow the typical client-server model. Users can use a REST client tool, such as Postman, to compose and submit requests to the RAMP API resources. For security, requests to the RAMP APIs must be submitted using HTTPS. Any language may be used to access the API for example, Python, Perl, Javascript, Java, C++ and so on.

RAMP REST APIs are closely aligned with the presentation of its UI. Currently, RAMP provides APIs for key functional areas within the UI including Authentication/Authorization, Fault Management (FM), Performance Management (PM), and License Management (LM) functions. Ribbon plans to expand RAMP API support in subsequent releases.

## Accessing the API Documentation from RAMP

The RAMP provides access to its primary API documentation directly from the RAMP UI. This comprehensive API specification is comprised of a set of definition files ( `.yaml files` ) each corresponding to a functional area within RAMP, such as PM Collection Profiles, LM Features, FM Notifications, and so on. Users select a file based on the type of operations they want to perform. When selected, the file contents appear within a user interface.

Each file contains a listing of the methods and resource paths provided to submit specific requests for the selected functional area. Click on an entry in the list to see details on the required parameters and structure for the related request and responses. The listing of requests is followed by detailed schema definitions for the objects within the requests/responses.

## View RAMP API User Documentation

To select and display an API definition file within a user interface:

### Start

1. Log on to the RAMP UI.
2. On the right side of the top bar, click **Menu**.
3. In the menu, select **REST API Documentation** to open the API documentation interface. By default, the definition file for **Authentication & Authorization** opens.
4. In the **Select a definition** list, the full list of definition files appears in alphabetical order. Select the file you want to open.
5. Click within the interface to expand sections to get more details on selected requests or schemas.

Note that RAMP uses the OpenAPI (Swagger) user interface to display the API definition files. Refer to <https://swagger.io/tools/swagger-ui/> for more information on using the Swagger UI.

## Download RAMP API Definition Files

To view or download the definition ( `.yaml` ) file contents so you can use it in another environment or with another API tool:

### Start

1. Complete the steps in the previous section to open a selected API file. The path to the selected file appears at the top of the page. For example, in the following figure, the path (in blue) is:  
`/auth/v1.0/discovery/getyaml/FM/fm-view-api.yaml`  

2. To view the file, click on the path. The source file opens in a separate tab.
3. To download the file, right-click on the path and select **Save as** and select a location on your system where you want to save a copy of the file.

## Authentication Requirements

To ensure that only authenticated users can use the API, users must submit credentials to request an authentication token from RAMP. The user must include this token in an Authorization header in each subsequent API request. Refer to [Example API Requests and Responses](#) to see how the authentication token is included in a request.

By default an authentication token expires in 15 minutes, but a user can request to refresh the token to continue submitting requests within the same session. Note that the duration before an authentication token expires is configurable within Authentication & Authorization admin settings.

Users can obtain authentication tokens using the below three ways.

- Using a Username and Password.
- Using a SAML service provider.
- Using a certificate.

## Obtain a Token Using a Username and Password

A user can submit an API request to receive an authentication token by submitting a valid RAMP username and password in a request. RAMP returns an authentication token in its response. The user includes this authentication token in subsequent API requests to authenticate the request.

| Method | URI                                                            | Body                                                            |
|--------|----------------------------------------------------------------|-----------------------------------------------------------------|
| POST   | https://<RAMP IP address or domain>/auth/v1.0/session/password | {<br>"username": "<username>",<br>"password": "<password>"<br>} |

## Obtain a Token using a SAML Service Provider

For deployments that have implemented a Security Assertion Markup Language (SAML)-based security realm, users can log into their SAML service provider and obtain an access token. The user then submits an API request for an authentication token that includes the SAML access token. RAMP returns an authentication token in its response. The user includes this authentication token in subsequent API requests to authenticate the request.

| Method | URI                                                               | Query Parameter | Body                               |
|--------|-------------------------------------------------------------------|-----------------|------------------------------------|
| POST   | https://<RAMP IP address or domain>/auth/v1.0/session/accessToken | tokentype=saml  | {<br>"token" : "<SAML token>"<br>} |

## Obtain a Token using a Certificate

For deployments that have imported or added certificates, the users can log into RAMP using certificate and obtain an access token. The user submits an API request for an authentication token that includes the certificate as a token part of request body. The RAMP returns an authentication token in its response. The user includes this authentication token in subsequent API requests to authenticate the request.

| Method | URI                                                                                | Body                                      |
|--------|------------------------------------------------------------------------------------|-------------------------------------------|
| POST   | https://<RAMP IP address or domain>/auth/v1.0/session/accessToken?type=certificate | {<br>"token" : "<certificate token>"<br>} |

When using Third-Party CA signed certificates, ensure that you have imported the CA certificate as well along with the certificate that you are using to get an authentication token. For more information, refer to [Importing Third Party Certificates](#).

## Refresh an Authentication Token

To continue a session for longer than the 15 minutes expiration for authentication tokens, before the token expires, a user can request to refresh the token. RAMP returns a new authentication token in its response. The user includes the new authentication token in subsequent API requests to authenticate the request.

| Method | URI                                                                                                                                                                               | Body                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| PUT    | <a href="https://&lt;RAMP IP address or domain&gt;/auth/v1.0/session/password/sessionToken">https://&lt;RAMP IP address or domain&gt;/auth/v1.0/session/password/sessionToken</a> | <pre>{   "token" : "&lt;token&gt;" }</pre> |

## Role-Based User Access Requirements

Role-based user access rules apply when submitting API requests to RAMP. The user account used to obtain the authentication token must have the same permission level as a user must have to complete the operation with the RAMP UI. The API definition files include information on the user privilege level required to submit different types of requests.

## Terminating a Session

Although tokens eventually expire, security best practice is to submit a request to logout and terminate a session.

| Method | URI                                                                                                                                   | Body                                  |
|--------|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| DELETE | <a href="https://&lt;RAMP IP address or domain&gt;/auth/v1.0/session">https://&lt;RAMP IP address or domain&gt;/auth/v1.0/session</a> | <current authentication token string> |

## Example API Requests and Responses

In this section:

- [User Authentication Using a Password](#)
  - [Request Contents](#)
  - [Successful Response](#)
  - [User Authentication Using a Certificate](#)
- [Retrieve the List of User Roles](#)
  - [Request Contents](#)
- [Add a Collection Profile](#)
  - [Request Contents](#)
- [Change Collection Profile Assignment](#)
  - [Successful Response Example](#)
  - [Retrieve RAMP License Keys](#)
  - [Request Contents](#)
- [Retrieve Usage Level for a Licensed Feature](#)
  - [Request Contents](#)
- [Configure OSS Trap Resync Parameters](#)
  - [Request Contents](#)
  - [Successful Response](#)

Related articles:

- [REST API Documentation](#)

The following sections contain examples of RAMP API requests and responses to illustrate the typical contents. Many methods and tools are available to work with REST APIs; therefore, your format may differ depending on your specific environment. Note that in the examples, tokens are shortened for readability.

## User Authentication Using a Password

In this example, a log on request is sent to the RAMP with a valid username and password for a user in the local authentication realm.

### Request Contents

**Request Method:** POST

**Request URI:** `https://<RAMP IP address>/auth/v1.0/session/password`

**Headers:**     Accept: application/json, application/javascript, text/javascript, text/json  
                  Content-Type: application/json; charset=UTF-8

**Request Body:**

```
{

 "username": "string",
 "password": "string"

}
```

### Curl Example

```
curl -k -i --request POST --location 'https://<RAMP IP address>/auth/v1.0/session/
password' \
--header 'Accept: application/json, application/javascript, text/javascript, text/json'
\
--header 'Content-Type: application/json' \
--data '{

 "username": "admin",
 "password": "admin"

}'
```

#### Note

The "-k" option is required if you are using the default RAMP certificate which is insecure but won't be necessary after you install your own certificate. Refer to [Secure Login to the RAMP GUI](#) for information on adding certificates to your system.

The "-i" option displays the response headers.

## Successful Response

```
HTTP/1.1 200
Date: Thu, 27 Oct 2021 18:37:26 GMT
Content-Type: application/json

{
 "token": "eyJhbGciOiJSUzI1NiJ9 ... yPvtfeXx9L05QkD1LIqT3JuA"
}
```

## User Authentication Using a Certificate

In this example, a log on request is sent to the RAMP using a certificate. A successful response returns an authentication token.

### Request Contents

**Request Method:** POST

**Request URI:** `https://<RAMP IP address>/auth/v1.0/session/accessToken?type=certificate`

**Headers:**     Accept: application/json, application/javascript, text/javascript, text/json  
              Content-Type: application/json; charset=UTF-8

**Request Body:**

```
{
 "token": "MIIFXjCCA0agAw ... zmZQqgB7CwxVI4HhvVOA=="
}
```

## Curl Example

```
curl -k -i --request POST --location 'https://<RAMP IP address>/auth/v1.0/session/accessToken?type=certificate' \
--header 'Accept: application/json, application/javascript, text/javascript, text/json' \
--header 'Content-Type: application/json' \
--data '{
```

```
"token":"MIIFXjCCA0agAw ... zmZQqgB7CwxVI4HhvVOA=="
}'
```

The "-k" option is required if you are using the default RAMP certificate, which is insecure but is not necessary after you install your own certificate. Refer to [Secure Login to the RAMP GUI](#) for information on adding certificates to your system. The "-i" option displays the response headers.

### Successful Response

```
HTTP/1.1 200
Date: Mon, 29 Jul 2024 10:33:46 GMT
Content-Type: application/json
{"token":"eyJhbGciOiJSUzI1NiJ9 ... XZ8PcjHsj2awnvGg"}
```

## Retrieve the List of User Roles

This example is to retrieve a request to retrieve information on the currently configured list of user roles.

### Request Contents

**Request Method:** GET

**Request URI:** `https://<RAMP IP address>/auth/v1.0/config/roles`

**Headers:**     **Authorization:** *<authentication token returned after successful authentication>*  
                   **Accept:** application/json, application/javascript, text/javascript, text/json  
                   **Content-Type:** application/json; charset=UTF-8

### Curl Example

```
curl --request GET --location 'https://<RAMP IP address>/auth/v1.0/config/roles' \
--header 'Authorization: eyJhbGciOiJSUzI1NiJ9 ... yPvtfeXx9L05QkD1LIqT3JuA1' \
--header 'Accept: application/json, application/javascript, text/javascript, text/json' \
--header 'Content-Type: application/json'
```

### Successful Response



HTTP/1.1 200

Date: Thu, 27 Oct 2021 18:47:26 GMT

Content-Type: application/json

```
[
 {
 "id": "1001",
 "name": "admin",
 "description": "admin role",
 "tenantId": "38400000-8cf0-11bd-b23e-10b96e4ef00d",
 "tenantName": "root"
 },
 {
 "id": "1003",
 "name": "calea",
 "description": "calea role",
 "tenantId": "38400000-8cf0-11bd-b23e-10b96e4ef00d",
 "tenantName": "root"
 },
 {
 "id": "1002",
 "name": "default",
 "description": "default role",
 "tenantId": "38400000-8cf0-11bd-b23e-10b96e4ef00d",
 "tenantName": "root"
 }
]
```

## Add a Collection Profile

In this example, a request to create a new Performance Management collection profile is given for collecting performance management statistics for a specified type of managed device:

### Request Contents

**Request Method:** POST

**Request URI:** https://<RAMP IP address>/collection-service/v1/collection

**Headers:** Authorization: <authentication token returned after successful authentication>  
Accept: application/json, application/javascript, text/javascript, text/json  
Content-Type: application/json; charset=UTF-8

**Request Body:**

```
[
 {
 "id": "string",
 "name": "string",
 "deviceType": "string",
 "deviceDisplayType": "string",
 "interfaceType": "string",
 "generationFreq": "string",
 "collectionFreq": "5",
 "overrides": number,
 "devicesAssoc": number,
 "isDefault": boolean,
 "statistics": [
 {
 "id": "string",
 "name": "string",
 "deviceType": "string",
 "deviceDisplayType": "string",
 "generationStatus": boolean,
 "generationFreq": "string",
 "collectionStatus": boolean,
 "collectionFreq": "string",
 "aggregationStatus": boolean,
 "isOverride": boolean,
 "mandatory": boolean
 }
]
 }
]
```

## Curl Example

```
curl --request POST --location 'https://<RAMP IP address>/collection-service/v1/
collection' \
--header 'Authorization: eyJhbGciOiJSUzI1NiJ9 ... yPvtfeXx9L05QkD1LIqT3JuA1' \
--header 'Accept: application/json, application/javascript, text/javascript, text/json' \
--header 'Content-Type: application/json' \
--data '{
 "id": null,
 "name": "Edge_SFTP",
 "deviceType": "EDGE",
 "deviceDisplayType": null,
 "interfaceType": "SFTP",
 "generationFreq": "5",
 "collectionFreq": "5",
 "overrides": null,
```

```
"devicesAssoc": null,
"isDefault": null,
"statistics": [
{
 "id": "EdgeSBCChannelStatusStats",
 "name": "SBCEDGEChannelStatusStats",
 "deviceType": "EDGE",
 "deviceDisplayType": "SBC Edge",
 "generationStatus": true,
 "generationFreq": "5",
 "collectionStatus": true,
 "collectionFreq": "5",
 "aggregationStatus": false,
 "isOverride": false,
 "mandatory": false
},
{
 "id": "EDGESBCEDGENWDLLicenseStats",
 "name": "SBCEDGENWDLLicenseStats",
 "deviceType": "EDGE",
 "deviceDisplayType": "SBC Edge",
 "generationStatus": true,
 "generationFreq": "5",
 "collectionStatus": true,
 "collectionFreq": "5",
 "aggregationStatus": false,
 "isOverride": false,
 "mandatory": true
},
{
 "id": "EDGESBCEDGEPTStats",
 "name": "SBCEDGEPTStats",
 "deviceType": "EDGE",
 "deviceDisplayType": "SBC Edge",
 "generationStatus": true,
 "generationFreq": "5",
 "collectionStatus": true,
 "collectionFreq": "5",
 "aggregationStatus": false,
 "isOverride": false,
 "mandatory": false
}
]
}'
```

## Successful Response

HTTP/1.1 200

Date: Thu, 27 Oct 2021 18:39:26 GMT

## Change Collection Profile Assignment

In this example, a request to change the Performance Management collection profile assignment for a specified device. Use an array to specify changes for more than one device.

The identifiers for nodes, clusters, and profiles can be returned using a GET for collection-assignments,

### Request Contents

**Request Method:** PUT

**Request URI:** `https://<RAMP IP address>/collection-service/v1/collection-assignments`

**Headers:** Authorization: <authentication token returned after successful authentication>  
Accept: application/json, application/javascript, text/javascript, text/json  
Content-Type: application/json; charset=UTF-8

**Request Body:**

```
[
 {
 "id": number,
 "clusterId": "string",
 "nodeId": number,
 "oldCollectionProfileId": number,
 "newCollectionProfileId": number,
 "collectionStatus": boolean
 }
]
```

### Curl Example

```
curl --request POST --location 'https://<RAMP IP address>/collection-service/v1/
collection-assignments' \
--header 'Authorization: eyJhbGciOiJSUzI1NiJ9 ... yPvtfeXx9L05QkD1LIqT3JuA1' \
--header 'Accept: application/json, application/javascript, text/javascript, text/json' \
--header 'Content-Type: application/json' \
--data '[
 {
 "id": 545,
 "clusterId": null,
 "nodeId": 10001,
 "oldCollectionProfileId": 306,
 "newCollectionProfileId": 1632,
```

```
 "collectionStatus": true
 }
]
```

## Successful Response Example

```
HTTP/1.1 200
```

```
Date: Thu, 27 Oct 2021 18:39:26 GMT
```

## Retrieve RAMP License Keys

The following example shows a request to retrieve the RAMP node-locked (legacy) and domain-locked (pubic) license keys that are required when generating a license:

## Request Contents

**Request Method:** GET

**Request URI:** `https://<RAMP IP address>/lm/v1.0/keys`

**Headers:**     **Authorization:** *<authentication token returned after successful authentication>*  
                  **Accept:** application/json, application/javascript, text/javascript, text/json  
                  **Content-Type:** application/json; charset=UTF-8

### Curl Example

```
curl --request GET --location 'https://<RAMP IP address>/lm/v1.0/keys' \
--header 'Authorization: eyJhbGciOiJSUzI1NiJ9 ... yPvtfeXx9L05QkD1LIqT3JuA1' \
--header 'Accept: application/json, application/javascript, text/javascript, text/json' \
--header 'Content-Type: application/json'
```

## Successful Response

```
HTTP/1.1 200
```

```
Date: Thu, 27 Oct 2021 18:42:26 GMT
```

```
Content-Type: application/json
```

```
{
 "legacy": [
```

```
"85416452d65941b8b0ee3d442cd31c48"
],
"public": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsc5/G+sZl/
Me88wboDimLGuWgoSQQcP37at0N00BcICgTYC6dD7KuUzsVjGsTfUe5+F7EwUoXn4eG1/
tBs1h794l7MzExsAr9HyDZHC0mQJAmA7Fk9bxYQjdYK0uBa9xTelGnq3yL9TXR6m4djKLWWeV4QXHuLxoV0yPbF1
1ozHtCeK1lEBJ3Ciayw5EICVWJwknjHWzmfflX940BlzbH2F8GSXGqogkkoLKfTC0t8fcuzZ/
X2+ZYYx4MUHoUhSrDykmDQUdd+PX+eSxDUM6B3lepIHBrevSLSBsDe/NM3DyhI9o02o0h7Jf4u5Gb2h8/
yBn76bySjKm2jRQHN2hJQIDAQAB"
}
```

## Retrieve Usage Level for a Licensed Feature

In this example, a request to retrieve the average usage of a specified feature during a specified time range. The feature is defined as a path parameter ("SBC-POL-RTU-D") and the time range is specified as query parameters (epoch time):

### Request Contents

**Request Method:** GET

**Request URI:** `https://<RAMP IP address>/lm/v1.0/feature/licenses/<feature ID>/chart/averageusage?epochStart=<start time>&epochEnd=<end time>`

**Headers:**     Authorization: <authentication token returned after successful authentication>  
                  Accept: application/json, application/javascript, text/javascript, text/json  
                  Content-Type: application/json; charset=UTF-8

### Curl Example

```
curl --request GET --location 'https://<RAMP IP address>/lm/v1.0/feature/licenses/SBC-
POL-RTU-D/chart/averageusage?epochStart=1633629119000&epochEnd=1633632720000' \
--header 'Authorization: eyJhbGciOiJIUzI1NiJ9 ... yPvtfeXx9L05QkD1LIqT3JuA1' \
--header 'Accept: application/json, application/javascript, text/javascript, text/json' \
--header 'Content-Type: application/json'
```

### Successful Response

HTTP/1.1 200

Date: Thu, 27 Oct 2021 18:42:26 GMT

Content-Type: application/json

## Configure OSS Trap Resync Parameters

In this example, a request to configure parameters for re-synchronizing traps with an Operation Support System (OSS). Depending on the SNMP version, different parameters are configured. This example shows configuration for SNMP v2.

### Request Contents

**Request Method:** POST

**Request URI:** `https://<RAMP IP address>/trap-resync-service/v1.0/trap-resync-setting`

**Headers:**     **Authorization:** *<authentication token returned after successful authentication>*  
                  **Accept:** application/json, application/javascript, text/javascript, text/json  
                  **Content-Type:** application/json; charset=UTF-8

**Request Body:**

```
{
 "snmpVersion": "string",
 "ossIpAddress": "string",
 "snmpWriteCommunity": "string",
 "securityName": "string",
 "securityLevel": "string",
 "authenticationProtocol": "string",
 "authenticationPassphrase": "string",
 "privacyProtocol": "string",
 "privacyPassphrase": "string"
}
```

### Curl Example

```
curl --request POST --location 'https://<RAMP IP address>/trap-resync-service/v1.0/trap-resync-setting' \
--header 'Authorization: eyJhbGciOiJIUzI1NiJ9 ... yPvtfeXx9L05QkD1LIqT3JuA1' \
--header 'Accept: application/json, application/javascript, text/javascript, text/json' \
--header 'Content-Type: application/json' \
--data '{
 "snmpVersion": "V2",
 "ossIpAddress": "1.2.3.4",
 "snmpWriteCommunity": "community123",
 "securityName": null,
 "securityLevel": null,
 "authenticationProtocol": null,
 "authenticationPassphrase": null,
```

```
"privacyProtocol": null,
"privacyPassphrase": null
'
```

## Successful Response

HTTP/1.1 200

Date: Thu, 27 Oct 2021 18:40:26 GMT

Content-Type: application/json



# RAMP Release Information

## Contents

- [Ribbon Application Management Platform 24.12R0 Release Notes](#)
  - [New in RAMP 24.12.00R000](#)

The RAMP release notes provide up-to-date information about product enhancements and changes, plus installation, upgrade and other pertinent details for each software release.

## Ribbon Application Management Platform 24.12R0 Release Notes

## Contents

- [About Ribbon Application Management Platform Release Notes](#)
  - [Release Notes Use and Distribution](#)
  - [Associated Ribbon Announcements](#)
- [Ribbon Application Management Platform](#)
  - [Compatibility with Ribbon Products](#)
- [New Features and Functionalities](#)
  - [New Features in Release 24.12.00R000](#)
  - [New Features in Previous Releases](#)
- [SOAP API Deprecation Notice](#)
- [Security Vulnerabilities](#)
- [Hardware and Software Requirements](#)
  - [Software Bundles](#)
  - [Ribbon OEM Host Operating System \(ROHOS\)](#)
  - [App Service](#)
- [Upgrade Notes](#)
- [Migration Notes](#)
- [Checksums and ID Details](#)
- [Resolved Issues](#)
  - [RAMP 24.12.00R000](#)
  - [RAMP 24.09.00R001](#)
- [Known Issues](#)
- [Known Limitations](#)

## About Ribbon Application Management Platform Release Notes

This document describes new features, latest hardware and software requirements, known limitations and other pertinent release information for the latest release of the Ribbon Application Management Platform.

**Note**

All Ribbon bugs reported by the customers on a given software release are fixed in the latest release of that software release branch.

To view and download the latest End of Product Sale (EoPS) and other End Of Life (EOL) notices, open a web browser and navigate to the Resource Library on the corporate website (<https://ribboncommunications.com/company/get-help/resource-library>)

## Release Notes Use and Distribution

Ribbon product release notes are protected under the copyright laws of the United States of America. This work contains proprietary information of [Ribbon Communications](#). Use, disclosure or reproduction in any form is strictly prohibited without prior authorization from [Ribbon Communications](#).

## Associated Ribbon Announcements

The following Ribbon announcements (formerly known as WBAs) are referenced in this release note:

**Warning-24-000008211:** FM process restart issue post switchover in the RAMP GR.

**Note:** If you use RAMP GR on a pre-23.12 release, apply this WBA and upgrade to 24.12R0.

**To view/subscribe to announcements (Warnings, Bulletins, Alerts, or PCNs):**

1. [Click here](#) to go to the "Announcements" page in the Ribbon Support Portal.
2. Enter the announcement number (last eight numbers) in the search field and click the magnifying glass icon (or press **Return**). You can alternatively use the filter tools located on the left side of the screen to narrow your search.

## Problems or Questions

For problems or questions, contact the Global Support Assistance Center:

**Ribbon Support Portal:** <https://ribboncommunications.com/services/ribbon-support-portal>

**Voice:** +1-833-RIBBON1 (1-833-742-2661)

## Ribbon Application Management Platform

The Ribbon Application Management Platform (RAMP) provides a centralized, cloud-optimized solution for the efficient management of every Ribbon element in a customer's network. RAMP provides a complete Fault, Configuration, Accounting, Performance, and Security solution with a robust portfolio of management and provisioning tools that allow service providers and enterprises to easily perform management of their network, quickly remediate issues, leading to an improved customer experience and reduced costs.

## Compatibility with Ribbon Products

Refer to the [Ribbon Application Management Platform Interoperability Matrix](#) for the latest and minimum compatible product versions supporting this release.

**Ribbon Elements Supported**

- Application Server

- Centralized Policy and Routing Server (PSX), and PSX Software Edition (PSX SWe)
- C20 Call Session Controller
- C3 Call Controller
- Data stream Integrator (DSI)
- Dell Servers
- Diameter Signaling Controller (DSC)
- Edge 8000
- EdgeMarc
- General Media Server ( GMS)
- G5 Line Access Gateway
- G6 Universal Gateway
- G9 Media Gateway
- Layer 2 Manager (L2MGR)
- Multimedia Resource Function Processor (MRFP)
- Ribbon Media Gateway (GSX9000)
- Session Border Controller Software Edition (SBC SWe)
- Session Border Controller 5400
- Session Border Controller 7000
- Session Border Controller CNe
- Session Border Controller SWe Edge
- Session Border Controller 1000
- Session Border Controller 2000
- Signaling Gateway (SGX4000)
- SIP Load Balancer

**Note**

In the RAMP 24.12 GUI or documentation, any instance of the SBC Core refers to **SBC 7000/5400/SWe/CNe** and **MRFP** products, unless otherwise noted. Any instance of the SBC Edge refers to the **SBC1000/2000** and **SBC SWe Edge**.

**Note**

The following table lists the supported/unsupported EdgeMarc Subtypes:

**Supported EdgeMarc Subtypes**

- 302
- 304
- 2900
- 2900A
- 2900E
- 2900PoE
- 4550v2
- 4551
- 4552
- 4555
- 4600T4
- 4601
- 4603
- 4604T4
- 4608PoE
- 4700
- 4701
- 4750
- 4751
- 4800
- 4808
- 4806v2
- 4808v2
- 4808
- 6000
- 7301
- 7400
- 8000

**Tip**

When upgrading your network, ensure to upgrade each product to the most current release to take advantage of the latest features, enhancements, and fixes.

## New Features and Functionalities

### New Features in Release 24.12.00R000

The New Features of RAMP 24.12.00R000 are available in:

- [New in RAMP 24.12.00R000](#)

**Note**

Beginning with the RAMP 24.12 release, the node-level postpaid reports are disabled by default, and the RAMP generates only the network-level postpaid reports. To enable the node-level postpaid reports, a new setting, "Generate Node-Level Postpaid Reports," is introduced to the LM administration page.

## New Features in Previous Releases

For the list of features in previous 24.09.xx releases, refer to the following release note:

- [New in RAMP 24.09R001](#)

## SOAP API Deprecation Notice

The RAMP SOAP API support for the SBC Core is only supported for EMS migrations to allow backwards compatibility. The RAMP SOAP API supports the SBC functionality through the SBC release 12.X. The functionality is targeted to deprecate in Q4 2024. Users need to migrate to the REST API for the SBC API access.

## Security Vulnerabilities

The following security vulnerabilities (CVEs) are fixed in this release:

**Note**

The severity is based on the CVSSv3.x scores. For more details about the individual CVE, refer to <https://nvd.nist.gov/vuln/search>. These are listed verified CVEs in 24.09R1 Release.

| Severity | CVE numbers                                                                                                                                                                                |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Critical | CVE-2022-42889, CVE-2022-42920                                                                                                                                                             |
| High     | CVE-2022-45688, CVE-2024-47554, CVE-2023-5072, CVE-2013-4002, CVE-2012-0881, CVE-2022-25647                                                                                                |
| Medium   | CVE-2021-29425, CVE-2020-13956, CVE-2022-45146, CVE-2015-5262, CVE-2020-14338, CVE-2022-23437, CVE-2009-2625, CVE-2023-2976, CVE-2015-5262, CVE-2021-38153, CVE-2024-29857, CVE-2024-30171 |
| Low      | CVE-2020-8908                                                                                                                                                                              |

## Hardware and Software Requirements

This section provides information about any release-specific Ribbon Application Management Platform software requirements.

### Note

- RAMP 24.12.00R000 is minimum supported on 16 vCPU. Contact Ribbon Support team for the upgrade-related assistance.
- The disk size is changed from 130GB to 150GB for the RAMP 23.09.00R000 and above releases. The templates are updated to reflect this change.
- Refer to the update, Warning-23-000007983.

## Software Bundles

Download the RAMP 24.12.00R000 software bundle from the Support Portal.

The following files are delivered as part of RAMP 24.12.00R000:

| Files                                                                                                                                                                                                       | Environment | Description                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------------------------------------|
| AMI ID = ami-0b7a556bed8551f04<br>AMI_NAME= release-ramp-v24.12.00r000-rhel-8.10.102-187-x86_64_580_12_10_24_16_42<br>templates.tar                                                                         | AWS         | RAMP install/upgrade on AWS          |
| AppServices-24.12.00R000-B7623_vmCCS-1.14.1-x86_64.qcow2<br>AppServices-24.12.00R000-B7623_vmCCS-1.14.1-x86_64.vmdk<br>AppServices-configDrive.img<br>heat_template_etcd.yml<br>AppServices-snmpMIBs.tar.gz | App Service | etcd deployment for auto switchover  |
| InsightAllMibs.tar                                                                                                                                                                                          | Generic     | MIB files                            |
| ramp-hostcheck-V24.12.00R000.tar.gz                                                                                                                                                                         | KVM         | Hostchecker tool for RAMP deployment |
| ramp-V24.12.00R000-RHEL-8.10.102-187-x86_64_580.img<br>ramp-V24.12.00R000-RHEL-8.10.102-187-x86_64_580-2024-12-10.vhd                                                                                       | Azure       | RAMP install/upgrade on Azure        |

| Files                                                                                                                                                                                                                                                               | Environment          | Description                                 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------------|
| ramp-V24.12.00R000-<br>RHEL-8.10.102-187-x86_64_580.qcow2<br>ramp-V24.12.00R000-<br>RHEL-8.10.102-187-<br>x86_64_580.qcow2.md5<br>templates.tar                                                                                                                     | OpenStack            | Image for RAMP install/upgrade on OpenStack |
| ramp-V24.12.00R000-<br>RHEL-8.10.102-187-x86_64_580.qcow2<br>ramp-V24.12.00R000-<br>RHEL-8.10.102-187-<br>x86_64_580.qcow2.md5<br>rampBootstrap-V24.12.00R000_RHEL.tar<br>configDriveImgDeployment.img                                                              | KVM                  | RAMP install/upgrade on KVM                 |
| ramp-V24.12.00R000-<br>RHEL-8.10.102-187-x86_64_580.vmdk<br>ramp-V24.12.00R000-<br>RHEL-8.10.102-187-<br>x86_64_580.vmdk.md5<br>ramp-V24.12.00R000-<br>RHEL-8.10.102-187-x86_64_580.ovf<br>configDriveImgDeployment.img<br>rampBootstrap-<br>V24.12.00R000_RHEL.tar | VMware               | RAMP install/upgrade on VMware              |
| ramp-V24.12.00R000-<br>rhv_ansible_playbooks.tar.gz<br>ramp-V24.12.00R000-<br>RHEL-8.10.102-187-x86_64_580.qcow2                                                                                                                                                    | RHV                  | RAMP install/upgrade on RHV                 |
| ramp-V24.12.00R000-SOL1-v361-<br>Generic.csar<br>ramp-V24.12.00R000-SOL1-v361-<br>marketplaceStructure.zip                                                                                                                                                          | VNFD                 | RAMP deployment with VNFM                   |
| rampBootstrap-V24.12.00R000_RHEL.tar                                                                                                                                                                                                                                | Migration<br>Upgrade | For the EMS to RAMP migration and upgrade   |

**Note**

- The 24.12.00R000 release supports deployment of the RAMP in Cloud Native Functionality (CNe). For the RAMP CNe installation/deployments, contact your Ribbon sales representative.
- If you are running the EMS/RAMP on the RHV platform, contact your Ribbon sales representative for upgrade/migration.

## Ribbon OEM Host Operating System (ROHOS)

The minimum ROHOS version and the Dell firmware versions compatible with the RAMP 24.12.00R000 release are provided below:

| ROHOS                           | Dell Firmware                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| 02.08.16 or higher <sup>1</sup> | <ul style="list-style-type: none"><li>• iDRAC: iDRAC9</li><li>• BIOS: 5.00.20.10</li><li>• Firmware: 2.17.1</li></ul> |
| Tested Version                  | VERSION=02.08.26<br>VERSION=02.08.23                                                                                  |

<sup>\*1</sup>For ROHOS versions higher than 02.08.16, refer to the [ROHOS Release Notes](#) for supported iDRAC, BIOS, and firmware versions.

## App Service

| Component | VNF                                                | CNF                     |
|-----------|----------------------------------------------------|-------------------------|
| RAMP      | 24.12.00R000-580                                   | 24.12.00R000-78         |
| ETCD      | AppServices-24.12.00R000-B7623_vmCCS-1.14.1-x86_64 | helm version: 1.4.0     |
|           |                                                    | bitnami/etcd: 3.5.16    |
|           |                                                    | bitnami/kubectl: 1.31.1 |
|           |                                                    | OBS: 3.2.2              |

**Key Changes:**

- Updated the OS patches
- update prometheus-autoconfig to 1.8.16
- update vmCCS to 1.14.1
- PLTF-5009: update third-party containers
  - Update etcd to 3.5.16



- Update prometheus to 2.54.1
- PLTF-5164: resize /dev/sda3 instead of /dev/sda2 after CommonOS added Secure Boot support

**Known Issues (VNF)**

None.

**Known Issues (CNe)**

None.

## Upgrade Notes

The following upgrade paths are supported in this release. The upgrade paths are supported for all platforms.

| Platform  | Release      |
|-----------|--------------|
| KVM       | 23.09.00R000 |
| VMware    | 23.12.00R000 |
| OpenStack | 24.03.00R001 |
| AWS       | 24.03.00R002 |
| Azure     | 24.06.00R000 |
| CNe       | 24.09.00R001 |

**Note**

To upgrade the RAMP from a pre-23.09 release , contact the Ribbon Support team.

## Migration Notes

The following migration paths are supported in this release.

| Platform  | EMS Release      |
|-----------|------------------|
| KVM       | 15.X, 14.x, 13.x |
| VMware    | 15.X, 14.x, 13.x |
| OpenStack | 15.X, 14.x, 13.x |
| AWS       | 15.X, 14.x, 13.x |

**Note**

Reach out to Ribbon Professional Service for more information about the EMS-to-RAMP Migration process.

**Note**

Current and last release Resolved and Known issues listed in this Release notes. For issues fixed in previous releases, refer to the corresponding Release Notes.

## Checksums and ID Details

The installation files have the following checksums:

| Md5sum                           | Size        | File Name                                                |
|----------------------------------|-------------|----------------------------------------------------------|
| c0f265374180cd3a299d5ab71fe53da4 | 14780521984 | ramp-V24.12.00R000-RHEL-8.10.102-187-x86_64_580.qcow2    |
| b8ece3e615364d00687d89530395944a | 5774573568  | AppServices-24.12.00R000-B7623_vmCCS-1.14.1-x86_64.qcow2 |
| 871d128944c1b7d52ff303df417a94f8 | 3265039360  | AppServices-24.12.00R000-B7623_vmCCS-1.14.1-x86_64.vmdk  |
| 33cec2c70bed47b48f6353cbeb481a32 | 131072      | AppServices-configDrive.img                              |
| e27f843d9727593eb26cb79e0f717c37 | 24627       | AppServices-snmpMIBs.tar.gz                              |
| 724603e22dd54cf419d50318c3145391 | 1048576     | configDriveImgDeployment.img                             |
| acc64f3b7d95ec50467a2bf503842358 | 77199360    | InsightAllMibs.tar                                       |
| 97ed0a5f26231c5df275381a12c2b24e | 3553280     | rampBootstrap-V24.12.00R000_RHEL.tar                     |
| 0f22ab584e6f22115386acaecdcdfe8f | 1914212     | ramp-hostcheck-V24.12.00R000.tar.gz                      |
| 145b8aa219397af33b12bbd64760fc56 | 5552        | ramp-V24.12.00R000-RHEL-8.10.102-187-x86_64_580.ovf      |
| 236eb06538c5d59e4d994c2ca49f4317 | 14456016384 | ramp-V24.12.00R000-RHEL-8.10.102-187-x86_64_580.vmdk     |

| Md5sum                           | Size        | File Name                                             |
|----------------------------------|-------------|-------------------------------------------------------|
| f32f50aed4de55c39fcbafd25fad2351 | 1879959     | ramp-V24.12.00R000-rhv_ansible_playbooks.tar.gz       |
| 53fba3a2c36dbcb1b8e5f4ee55f253a5 | 3122519     | ramp-V24.12.00R000-SOL1-v361-Generic.csar             |
| 43e6124ee3bac66b57500909452db1df | 14640409432 | ramp-V24.12.00R000-SOL1-v361-marketplaceStructure.zip |
| 8f60a4abc2fea4bb563d8ed6858b9029 | 254023680   | sbc_api_doc_v12_01.04.tar                             |
| aced8c67dcce85cf1cc0258aeacef17d | 153600      | templates.tar                                         |
| baa38a69492539bbdc429f36d7c00804 | 50822       | heat_template_etcd.yml                                |
| e8619a62987dedc171321ca27d4aa0ab | 133635829   | testTools-V24.12.00R000.tar.gz                        |

## Resolved Issues

### RAMP 24.12.00R000

The following issues are resolved in RAMP 24.12R0 release:

#### Severity 1 Issue

The following table lists the resolved severity 1 issue in this release:

| Issue ID  | Original Issue | Sev | Problem Description                                              | Resolution                                                                                                                                                                                                       |
|-----------|----------------|-----|------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-10746 | NA             | 1   | Unable to run the STI signing and verification on the same call. | <b>Impact Statement:</b> Unable to perform the STI signing and verification on the same call.<br><b>Resolution Details:</b> The RAMP 24.12 is enhanced to support STI signing and verification on the same call. |

#### Severity 2 and 3 Issues

The following table lists the resolved severity 2 and 3 issues in this release:

| Issue ID  | Original Issue | Sev | Problem Description                                                                                                                            | Resolution                                                                                                                                                                                                                                                                            |
|-----------|----------------|-----|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-8977  | NA             | 3   | The RAMP displays database and Kafka exceptions when users open 50 event lists.                                                                | <b>Impact Statement:</b> N/A<br><b>Resolution Details:</b> Modified the code to handle the exceptions.                                                                                                                                                                                |
| AFM-9984  | NA             | 3   | The RAMP generates alarms for the Agent version mismatch.                                                                                      | <b>Impact Statement:</b> The RAMP generates the<br><code>sonusV2VfyMgrApplVersionFailNotification /</code><br><code>sonusV2VfyMgrAgentVersionFailNotification</code> alarms when the RAMP agent restarts.<br><b>Resolution Details:</b> Removed obsolete alarms to resolve the issue. |
| AFM-10048 | NA             | 3   | After implementing the relocateGR on the RAMP 23.09, the node turns offline, and relocation fails (Random occurrence).                         | <b>Impact Statement:</b> Unlock for the Peer fails due to the timeout, resulting in relocation failure.<br><b>Resolution Details:</b> Increased the timeout value to 600 seconds while performing the unlock operation.                                                               |
| AFM-10369 | NA             | 3   | The RAMP waits five minutes to display the failure status for the Device Backup job.                                                           | <b>Impact Statement:</b> The User must wait five minutes to see the failure status on the GUI.<br><b>Resolution Details:</b> Modified the code to handle the error scenarios and report the errors correctly.                                                                         |
| AFM-11142 | NA             | 3   | The Instanceup fails with the error, "Node is unregistered" when the SBC Direct Single node is started after it is unregistered from the RAMP. | <b>Impact Statement:</b> The Instanceup fails with the error, "Node is unregistered".<br><b>Resolution Details:</b> Modified the code to update both the node status and host status to "Partially Registered" status when the active node re-registers.                              |

| Issue ID  | Original Issue | Sev | Problem Description                                                                       | Resolution                                                                                                                                                                                                                                                                                                                                                                           |
|-----------|----------------|-----|-------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-11473 | NA             | 3   | Realign the Tab key usage flow for the User Creation screen.                              | <p><b>Impact Statement:</b> The Tab key usage flow to navigate the User Creation screen is not correctly aligned.</p> <p><b>Resolution Details:</b> Updated the form field elements to place the "username", "password", and "re-enter password" fields in one div element on the left hand side and the "tenant" and the "description" on the right-hand side.</p>                  |
| AFM-11581 | NA             | 2   | The GSX Navigator and Task Configuration buttons do not respond when the network is slow. | <p><b>Impact Statement:</b> The GSX Navigator and Task Configuration buttons use a flat styling without any hover or click effect. Because of this, the user could not tell if an operation (click) was happening, giving the impression that buttons were not responding when the network was slow.</p> <p><b>Resolution Details:</b> Removed the styling to resolve the issue.</p> |
| AFM-11788 | NA             | 3   | Document the etcd upgrade procedure with the RAMP upgrade procedure.                      | <p><b>Impact Statement:</b> The etcd upgrade procedure is not available.</p> <p><b>Resolution Details:</b> Documented the etcd upgrade procedure. For more information, refer to <a href="#">Upgrading etcd</a>.</p>                                                                                                                                                                 |
| AFM-11871 | NA             | 2   | The EdgeMarc PCAP and Diagnostic Snapshot do not work on the public IP address setup.     | <p><b>Impact Statement:</b> Certain EdgeMarc features were not working when deploying the EdgeMarc with a Public IP.</p> <p><b>Resolution Details:</b> Modified the code to resolve this issue.</p>                                                                                                                                                                                  |
| AFM-11918 | NA             | 2   | The PSX Manager <code>Jsonlp</code> file download failings after migrating to the RAMP.   | <p><b>Impact Statement:</b> The <code>proxyPreferredIp</code> value was missing after a migration, which caused a PSX Manager launch failure.</p> <p><b>Resolution Details:</b> Modified the code to resolve this issue.</p>                                                                                                                                                         |

| Issue ID  | Original Issue | Sev | Problem Description                                                         | Resolution                                                                                                                                                                                                                                                                                                                                                               |
|-----------|----------------|-----|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-11996 | NA             | 3   | Provide support in including "commas" in the exported PM CSV file.          | <b>Impact Statement:</b> The RAMP does not support including "commas" in the exported PM CSV file.<br><b>Resolution Details:</b> Modified the code to support including "commas" in the exported PM CSV file.                                                                                                                                                            |
| AFM-12033 | NA             | 3   | RAMP 24.06R0: Security scan vulnerability.                                  | <b>Impact Statement:</b> The RAMP reports vulnerabilities during the security scan.<br><b>Resolution Details:</b> Handled all the reported vulnerabilities.                                                                                                                                                                                                              |
| AFM-12035 | NA             | 3   | A missing line item for the SBC SWe Edge HA fails License Profile creation. | <b>Impact Statement:</b> When creating a license profile for the SBC SWe Edge, The user is unable to generate the license since the line item SBC-SWE-EDGE-INSTANCE-D contains a description that says, "SWeEdge HA is not available to select."<br><b>Resolution Details:</b> Modified the code to resolve the issue.                                                   |
| AFM-12075 | NA             | 3   | Allow the CLI session to the non-SSO SBC.                                   | <b>Impact Statement:</b> The RAMP user can log in through the CLI as an admin user to the older version of the SBCs (pre-11.1 versions) that do not support the SSO login.<br><b>Resolution Details:</b> Introduced new property to both configuration file and User Interface to choose whether to enable/disable CLI access to older non-SSO SBCs based on deployment. |

| Issue ID  | Original Issue | Sev | Problem Description                                                                         | Resolution                                                                                                                                                                                                                                                                                                                                                    |
|-----------|----------------|-----|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12098 | NA             | 2   | Data miss aligned in the RAMP Task Configurator IP Trunk Group.                             | <b>Impact Statement:</b> Data that is misaligned in the RAMP Task Configurator for Selected IP Trunk Group displays incorrect data for certain fields.<br><b>Resolution Details:</b> Modified the code to prevent argument value misalignment when creating an IP TG while an empty argument is added to the task instance info,                              |
| AFM-12105 | NA             | 3   | Unable to dump the core files since the directory, <code>/home/core</code> does not exist.  | <b>Impact Statement:</b> The directory, <code>/home/core</code> is missing in the RAMP, which results in failure to store core files during unexpected crashes.<br><b>Resolution Details:</b> Added the missing directory to resolve the issue.                                                                                                               |
| AFM-12256 | NA             | 3   | The "Apply" and "OK" buttons perform the same functionality in the RAMP GUI.                | <b>Impact Statement:</b> The functionality of the "Apply" and "OK" buttons overlap.<br><b>Resolution Details:</b> Removed the "Apply" button from the Create Report Schedule form since it only applies to the Edit form.                                                                                                                                     |
| AFM-12286 | NA             | 3   | Add the <code>sonusHostDiskMonHardErrorNotification</code> alarm to the RAMP documentation. | <b>Impact Statement:</b> The <code>sonusHostDiskMonHardErrorNotification</code> alarm was not available in the RAMP documentation.<br><b>Resolution Details:</b> Added the <code>sonusHostDiskMonHardErrorNotification</code> alarm page to the RAMP documentation.<br>For more information, refer to <a href="#">sonusHostDiskMonHardErrorNotification</a> . |

| Issue ID  | Original Issue | Sev | Problem Description                                                                   | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------|----------------|-----|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12460 | NA             | 3   | The PM collection fails for the Edge nodes after migrating from the EMS to the RAMP.  | <p><b>Impact Statement:</b> The PM collection does not work on the Edge node after an EMS to RAMP migration.</p> <p><b>Resolution Details:</b> Added the missing <code>id_ecdsa.pub</code> key to the <code>~/.ssh/authorized_keys</code> entry for the Insight user. The EV uses this Insight user's SSH identity to connect to the SFTP without a password.</p>                                                                                                                                                                                                                                                                                   |
| AFM-12472 | NA             | 3   | Document the Character Limitation for the Profile Name.                               | <p><b>Impact Statement:</b> The Character limitation for the Profile Name was mentioned in the documentation.</p> <p><b>Resolution Details:</b> Updated the document with a note stating that the collection profile name must contain alphanumeric characters with a maximum length of 23. For more information, refer to <a href="#">Define Statistics to Collect</a>.</p>                                                                                                                                                                                                                                                                        |
| AFM-12484 | NA             | 3   | The RAMP generates an error message stating, "Password will Expire in -19898 day(s)." | <p><b>Impact Statement:</b> The user receives a password expiry message that prevents logging in to the system.</p> <p><b>Resolution Details:</b></p> <p>Modified the code to handle the scenario. With this resolution, when the user updates the LOCAL realm value for the password nonreusable time period and password aging, the following conditions are met.</p> <ul style="list-style-type: none"><li>• <code>PassHistPurgeBeforeTime</code><br/><code>&gt;=</code><br/><code>PassReusableTimePeriod</code></li><li>• <code>PassHistPurgeBeforeTime</code><br/><code>&gt;= PassAging &gt;=</code><br/><code>PassExpWarning</code></li></ul> |



| Issue ID  | Original Issue | Sev | Problem Description                                                                            | Resolution                                                                                                                                                                                                                                                                        |
|-----------|----------------|-----|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12496 | NA             | 3   | The PM CSV purger script generates authentication error.                                       | <b>Impact Statement:</b> Unable to implement the purger job for the CSV files.<br><b>Resolution Details:</b> Modified the script to run with the correct permissions.                                                                                                             |
| AFM-12498 | NA             | 3   | RAMP JITC/FIPS: The RAMP generates errors when running the JBoss CLI commands.                 | <b>Impact Statement:</b> The RAMP generates log errors while processing the JBoss CLI command. This error does not impact any RAMP functionality.<br><b>Resolution Details:</b> Modified the application to handle the error scenario.                                            |
| AFM-12507 | NA             | 2   | The RAMP SGX discovery function does not work properly                                         | <b>Impact Statement:</b> The SGX discovery fails after a switchover.<br><b>Resolution Details:</b> Modified the code to use the IPs of the second host.                                                                                                                           |
| AFM-12508 | NA             | 3   | Enhance the <code>analyzeSystem.sh</code> script.                                              | <b>Impact Statement:</b> If there are multiple interfaces with similar names, the script fails since it receives network information for multiple interfaces instead of receiving it for one interface.<br><b>Resolution Details:</b> Modified the script to handle the scenario. |
| AFM-12510 | NA             | 3   | Issue observed in Configuration Management Permission in Network Wide Provisioning Operations. | <b>Impact Statement:</b> The RAMP allows the user to perform provisioning, backup, and upgrade without holding the Configuration Management permission.<br><b>Resolution Details:</b> Modified the code to list the nodes based on the user role.                                 |

| Issue ID  | Original Issue    | Sev | Problem Description                                                                              | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|-------------------|-----|--------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12511 | NA                | 3   | The RAMP fails to query the server error for the AD user.                                        | <b>Impact Statement:</b> The RAMP fails to query the server error due to a missing step in the document.<br><b>Resolution Details:</b> Updated the document to add the missing step. For more information, refer to <a href="#">Post-Upgrade Procedures for RAMP</a> .                                                                                                                                                                                                                                         |
| AFM-12549 | NA                | 3   | Fields in the inventory report contain NULL for the primary SBC node name.                       | <b>Impact Statement:</b> The Inventory Report contains NULL for the primary SBC HA hostname.<br><b>Resolution Details:</b> Modified the code to set the correct hostname for the SBC HA.                                                                                                                                                                                                                                                                                                                       |
| AFM-12592 | NA                | 3   | Some of the commands fail in the GSX CLI through the RAMP.                                       | <b>Impact Statement:</b> The Incorrect role, gsx.prov, was used for an auth check when running these commands through the GSX CLI in the RAMP, resulting in provisioning failures.<br><b>Resolution Details:</b> Updated the role to devices.prov.                                                                                                                                                                                                                                                             |
| AFM-12595 | AFM-10338 (24.03) | 2   | The RAMP performed an automatic switchover due to a healthCheck failure on the InsightHotDeploy. | <b>Impact Statement:</b> Occasionally, the system resources memory/CPU goes high, which causes the Linux OOM killer to kick in and kill the INSIGHT JBoss process, initiating a SWACT.<br><b>Resolution Details:</b> To avoid a SWAT, the INSIGHT JBoss process's OOM score is reduced to "-300" whenever it is spawned. This ensures the Linux OOM killer does not pick the INSIGHT JBoss process, which avoids SWACT. Even if killed, the rest of the processes restart on the same instance within seconds. |

| Issue ID  | Original Issue      | Sev | Problem Description                                                                    | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------|---------------------|-----|----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12597 | NA                  | 2   | Gaps in the RAMP SBC HA communication when the SBC switchover results in node offline. | <p><b>Impact Statement:</b></p> <ol style="list-style-type: none"> <li>1. For a non-cloud SBC HA, when the active reboots, the automatic rediscovery fails for both hosts, and the node stays in a Registered - Offline state.</li> <li>2. For a cloud SBC, even though automatic rediscovery succeeds for the new active node after an SBC switchover, the primary IP address is not updated to the currently active host IP address, and the node stays in a Registered - Offline state.</li> </ol> <p><b>Resolution Details:</b> Modified the code to add a retry for the non-cloud SBC.</p> |
| AFM-12685 | NA                  | 2   | Improve the <code>manualBackup.sh</code> script.                                       | <p><b>Impact Statement:</b> A backup lasts a very long time because of the large number of parquet files collected in the backup.</p> <p><b>Resolution Details:</b> The code is modified to include an option to skip the PM parquet files during the backup.</p>                                                                                                                                                                                                                                                                                                                               |
| AFM-12761 | AFM-12521 (24.03R3) | 2   | The PM export fails in large networks with the "Argument list too long" error.         | <p><b>Impact Statement:</b> Failed to export the PM data to multiple locations when the number of devices are approximately 1500 and the device names are long.</p> <p><b>Resolution Details:</b> Modified the code to write the arguments to the file and pass the filename as an argument to the export script to avoid the "Argument list too long" error.</p>                                                                                                                                                                                                                               |
| AFM-12875 | NA                  | 3   | The RAMP installation on Azure generates an error on the first deployment.             | <p><b>Impact Statement:</b> Some steps in the customer documentation are not clear or are missing, causing a RAMP installation failure on Azure.</p> <p><b>Resolution Details:</b> Updated the document <a href="#">Instantiate a Standalone RAMP Instance on Azure</a>.</p>                                                                                                                                                                                                                                                                                                                    |

| Issue ID  | Original Issue | Sev | Problem Description                                                      | Resolution                                                                                                                                                                                                                                                                                                                               |
|-----------|----------------|-----|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12891 | NA             | 2   | The RAMP PM statistics are not visible in the OBF backend.               | <b>Impact Statement:</b> Missing PM data in the OBF.<br><b>Resolution Details:</b> Modified the code to successfully copy the PM metric <code>tarball</code> file from the RAMP to the telemetry-agent's PVC without permission issues.                                                                                                  |
| AFM-12933 | NA             | 3   | The ETCD CNF Health Check documentation update.                          | <b>Impact Statement:</b> Enhance the product documentation to include the ETCD CNF Health Check for CNF deployments.<br><b>Resolution Details:</b> Updated the product documentation. For more information, refer to <a href="#">RAMP CNF etcd Health Check</a> .                                                                        |
| AFM-12938 | NA             | 2   | RAMP CNF: RAMP FMaaS ETSI format update.                                 | <b>Impact Statement:</b> Enhance alarm mapping to use the ETSI format.<br><b>Resolution Details:</b> Enhanced alarm mapping to use the ETSI format.                                                                                                                                                                                      |
| AFM-12944 | NA             | 2   | The SBC API deployment failures cause a failure during the RAMP startup. | <b>Impact Statement:</b> The RAMP startup fails because some services do not come up within the stipulated timeframe.<br><b>Resolution Details:</b> Modified the code to start some services in the background and increase the timeout to avoid startup failures.                                                                       |
| AFM-12949 | NA             | 2   | The Node Lock License association is missing after a migration.          | <b>Impact Statement:</b> The Node Lock License association is missing after migrating from the EMS 14.1.6 to the RAMP 24.03.R2.<br><b>Resolution Details:</b> Modified the code to obtain all nodes from the Auth API on the first restart after a migration to prevent the LM service from starting early before the data is available. |

| Issue ID  | Original Issue      | Sev | Problem Description                                                                            | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------|---------------------|-----|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12951 | AFM-12489 (24.03R3) | 2   | The RAMP fails to generate SBC PMs for the configured remote destinations, SevOne, and RA.     | <b>Impact Statement:</b> Downstream was not receiving consistent PM data from the RAMP.<br><b>Resolution Details:</b> The code is updated to handle the scenario where the Export service does not copy files to the RA since the exporter-service is writing a Kafka message not present in the Kafka topic due to a race condition.                                                                                                                           |
| AFM-12984 | NA                  | 2   | RAMP 24.03R2: The RAMP fails to generate post-paid reports.                                    | <b>Impact Statement:</b> The RAMP is not receiving the post-paid reports, resulting in a report processing failure. The RAMP failed to send the report because an OOM occurred while processing the report.<br><b>Resolution Details:</b> Changed the design to fetch the data in the sample so that the LM fetches the one-day data in three iterations, writes it to a file and processes it. This design allows the processing of large data without an OOM. |
| AFM-13038 | NA                  | 2   | Errors observed in TrunkGroupSummaryReport, TotalConfiguredDSOs, and TotalEnabledDSOs columns. | <b>Impact Statement:</b> The RAMP fails to report the correct data to the user.<br><b>Resolution Details:</b> Modified the code to fetch and process the PM data correctly.                                                                                                                                                                                                                                                                                     |
| AFM-13094 | NA                  | 2   | Migration: localhost discovery fails post migration with different IP address and hostname.    | <b>Impact Statement:</b> The RAMP discovery fails with an error "Certificates do not conform to algorithm constraints".<br><b>Resolution Details:</b> The code is modified to restore the agent keystore from the EMS to RAMP if the keystore includes the MD5withRSA signature algorithm. If the CA-signed agent certificate is used, re-generate CSR the and re-import the certificate to the agent keystore.                                                 |

| Issue ID  | Original Issue | Sev | Problem Description                                                     | Resolution                                                                                                                                                                                                                                                                                   |
|-----------|----------------|-----|-------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-13198 | NA             | 3   | Update the documented procedure "Configure RAMP for TLS Communication". | <b>Impact Statement:</b> The missing steps prevented RAMP from pushing licensing data to the SBC for a JITC-enabled RAMP.<br><b>Resolution Details:</b> Updated the procedure with the required steps. For more information, refer to <a href="#">Configure RAMP for TLS Communication</a> . |

## RAMP 24.09.00R001

The following issue is resolved in RAMP 24.09R1 release:

### Severity 1 Issue

The following table lists the resolved severity 1 issue in this release:

| Issue ID  | Original Issue | Sev | Problem Description                           | Resolution                                                                                                                                            |
|-----------|----------------|-----|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| PLTF-4086 | N/A            | 1   | Security vulnerabilities in the RAMP (23.09). | <b>Impact Statement:</b> Security vulnerabilities are observed in various scans.<br><b>Resolution Details:</b> Resolved the critical vulnerabilities. |

### Severity 2 and 3 Issues

The following table lists the resolved severity 2 and 3 issues in this release:

| Issue ID | Original Issue | Sev | Problem Description                                                        | Resolution                                                                                                                                                                                                                                      |
|----------|----------------|-----|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-7376 | N/A            | 3   | The RAMP CLI does not disconnect after the configured idle timeout period. | <b>Impact Statement:</b> The CLI session stays active even after the configured idle timeout.<br><b>Resolution Details:</b> Modified the code to disconnect the EMS CLI session when the CLI inactivity exceeds the configured disconnect time. |

| Issue ID  | Original Issue | Sev | Problem Description                                                                                           | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|----------------|-----|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-7461  | N/A            | 2   | The RAMP GUI session does not expire when the user performs actions on the same page after a session timeout. | <b>Impact Statement:</b> The RAMP GUI session does not disconnect when users perform actions on a page after a session timeout.<br><b>Resolution Details:</b> Modified the code to log the user out on a session timeout.                                                                                                                                                                                                                                                                                                                                      |
| AFM-8412  | N/A            | 3   | Augment documentation for the ETCD operations.                                                                | <b>Impact Statement:</b> Missing ETCD documentation for detailed scenarios and commands to debug the system.<br><b>Resolution Details:</b> The following documents are updated: <ul style="list-style-type: none"><li>• <a href="#">Import Previously Generated TLS Certificate</a></li><li>• <a href="#">GSX Upgrade Automation</a></li><li>• <a href="#">RAMP GR Auto-Switchover Troubleshooting</a></li></ul>                                                                                                                                               |
| AFM-8493  | N/A            | 3   | The <code>jboss-cli.sh</code> script requires credentials for editing without enabling the FIPS.              | <b>Impact Statement:</b> The <code>jboss-cli.sh</code> script requires credentials to perform any operation.<br><b>Resolution Details:</b><br>Modified the code to enable silent authentication by default for the <code>jboss-cli.sh</code> . Also, included a script to disable the silent authentication.<br>Updated the following documents: <ul style="list-style-type: none"><li>• <a href="#">Configure Silent Auth for Jboss CLI</a></li><li>• <a href="#">Reset Admin Password for Jboss CLI</a></li><li>• <a href="#">Change Log Level</a></li></ul> |
| AFM-10328 | N/A            | 2   | Generate the CSR with RSA key size of 4096 bit.                                                               | <b>Impact Statement:</b> Users cannot generate a CSR with a key size of 2048 bits.<br><b>Resolution Details:</b> Modified the CSR configuration <code>manageCert</code> script to generate CSRs with a key size between 2048 and 4096 bits.                                                                                                                                                                                                                                                                                                                    |

| Issue ID  | Original Issue | Sev | Problem Description                                                            | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------|----------------|-----|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-10338 | N/A            | 3   | Automatic switchover occurs due to high Insight CPU usage (random occurrence). | <p><b>Impact Statement:</b> An automatic switchover occurs due to a high Insight CPU usage (random occurrence).</p> <p><b>Resolution Details:</b> The code is modified to reduce the memory usage in the FM, disable the <code>setroubleshootd</code> service, and reduce the Insight process OOM score to ensure the OOM killer does not pick it up in case of intermittent high system memory.</p>                                                                  |
| AFM-10393 | N/A            | 3   | The GSX timer-based alarm on the RAMP does not clear automatically.            | <p><b>Impact Statement:</b> A few alarms from the legacy devices do not clear automatically.</p> <p><b>Resolution Details:</b> Modified the code to support the timer alarms. These alarms clear automatically.</p>                                                                                                                                                                                                                                                   |
| AFM-10408 | N/A            | 2   | Certificate-based authentication for the REST API in the RAMP.                 | <p><b>Impact Statement:</b> Use the certificate-based authentication for the REST API in the RAMP.</p> <p><b>Resolution Details:</b> The product documentation is updated to provide more information on using certificate authentication for the REST APIs. For more information, refer to:</p> <ul style="list-style-type: none"> <li>• <a href="#">Example API Requests and Responses</a></li> <li>• <a href="#">Importing Third Party Certificates</a></li> </ul> |
| AFM-10511 | N/A            | 2   | The <code>HostSwapUsageRisingThreshold</code> alarm stays in the idle state.   | <p><b>Impact Statement:</b> The RAMP generates <code>HostSwapUsageRisingThreshold</code> alarm during an idle state.</p> <p><b>Resolution Details:</b> This is an expected Red Hat Linux behavior and does not affect any RAMP functionality. The severity of the alarm is reduced to "Informational".</p>                                                                                                                                                            |



| Issue ID  | Original Issue | Sev | Problem Description                                                                                                                                | Resolution                                                                                                                                                                                                                                                                                                                                     |
|-----------|----------------|-----|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-10560 | N/A            | 2   | The RAMP switchovers from Source to Target due to high CPU usage.                                                                                  | <b>Impact Statement:</b> The RAMP switches over due to high CPU usage.<br><b>Resolution Details:</b> Modified the code to reduce the memory usage in the FM. Disabled the <code>settroubleshootd</code> service and reduced the Insight process OOM score to ensure the OOM killer does not pick it up during intermittent high system memory. |
| AFM-10725 | N/A            | 2   | The RAMP fails to export all interval data to Ribbon Analytics.                                                                                    | <b>Impact Statement:</b> The RAMP fails to export all the interval data to the RA if the export time is extended.<br><b>Resolution Details:</b> Modified the code to schedule the failed tasks immediately instead of waiting for the next interval.                                                                                           |
| AFM-11097 | N/A            | 2   | RAMP 24.06: Cipher package Nessus scan vulnerabilities.                                                                                            | <b>Impact Statement:</b> Vulnerabilities are observed in various scans.<br><b>Resolution Details:</b> Resolved critical vulnerabilities.                                                                                                                                                                                                       |
| AFM-11229 | N/A            | 2   | Observed the <code>sonusV2VfyMgrApplVersionFailNotification / sonusV2VfyMgrAgentVersionFailNotification</code> alarm after migrating from the EMS. | <b>Impact Statement:</b> A few legacy VfyMgr alarms are present after migrating from the EMS.<br><b>Resolution Details:</b> Removed the legacy alarms since the RAMP automatically rediscovers a node if it goes offline and returns. These alarms are no longer needed.                                                                       |
| AFM-11355 | N/A            | 2   | RAMP support for all EdgeMarc devices.                                                                                                             | <b>Impact Statement:</b> A few EdgeMarc device versions were missed in the RAMP.<br><b>Resolution Details:</b> Added support for the EdgeMarc 7400 model.                                                                                                                                                                                      |

| Issue ID  | Original Issue | Sev | Problem Description                                                          | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|----------------|-----|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-11370 | N/A            | 3   | The RAMP fails to retain the Force Password Change option after a migration. | <p><b>Impact Statement:</b> The user settings of the Force Password Change option are not retained/updated after the migration from the EMS to the RAMP.</p> <p><b>Resolution Details:</b> The RAMP uses double negation to understand the EMS DB equivalent field, <code>exempt_aging</code> <code>forcepasswordchange</code> value in the RAMP. The EMS-mapped field is <code>password_change</code>. If the Force Password Change option is enabled on the EMS, <code>password_change</code> is 3 in the EMS DB. However, the RAMP migration script always mapped the field with <code>!= 0</code> and set it to "True" for the <code>forcepasswordchange</code>. An explicit check in the RAMP migration script is performed to check for the values and fix them.</p> |
| AFM-11378 | N/A            | 3   | Schema mismatch causing FM to restart after an upgrade from 23.09 to 24.03.  | <p><b>Impact Statement:</b> When the RAMP is upgraded from 23.09 to later versions, a Kafka message schema compatibility issue is observed, as the old schema is registered with the schema registry. This schema gets registered with the schema registry when the UI operations are performed on the alarms received from the SBC and the DSC.</p> <p><b>Resolution Details:</b> The fix for this issue is communicated through a bulletin and provided a patch to apply after the upgrade from 23.09 to 24.03 and before GR setup.</p>                                                                                                                                                                                                                                  |
| AFM-11381 | N/A            | 3   | The RAMP GUI TLS certificate (2k vs 4k).                                     | <p><b>Impact Statement:</b> The user cannot generate the CSR with a key size greater than 2048.</p> <p><b>Resolution Details:</b> The script <code>manageCert</code> is modified to support the CSR generation with a key size between 2048 and 4096 bits. The key size is configurable in the CSR configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Issue ID  | Original Issue | Sev | Problem Description                                                                        | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|----------------|-----|--------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-11473 | N/A            | 2   | Modify the User Creation tab to make it more user-friendly.                                | <p><b>Impact Statement:</b> After entering the password in the Password field, the user must press the Tab key multiple times to navigate to the <b>Re-Enter Password</b> field.</p> <p><b>Resolution Details:</b> Changed the form field elements to place the Username, Password, and Re-Enter Password fields in the left div and <b>Tenant</b> and <b>Description</b> fields in the right div.</p>                                                                                                                                                                                      |
| AFM-11573 | N/A            | 2   | Duplicated Resource Groups are present in the user Interface.                              | <p><b>Impact Statement:</b> Duplicated Resource Groups are present in the user interface.</p> <p><b>Resolution Details:</b> Modified the code to disable the <b>Save</b> button once it is clicked and enable when the API response is complete.</p>                                                                                                                                                                                                                                                                                                                                        |
| AFM-11638 | N/A            | 3   | The RAMP fails to populate the Trunk Group when selecting the Daily PM.                    | <p><b>Impact Statement:</b> The PSTN Index/trunk group name is not loaded in the PM reports page when the user selects the granularity "Hourly" for GSX Nodes.</p> <p><b>Resolution Details:</b> The user's parquet included data with empty trunk group names. The <code>dropna</code> method call on the dataframe did not/ will not remove these empty columns/rows. Hence, <code>getIndexValues.py</code> returned an empty <code>trunkgroupname</code> for all PSTN Indexes. Replaced the empty strings with 'NaN' values so that the <code>dropna</code> method drops those rows.</p> |
| AFM-11653 | N/A            | 3   | The PM Administration fails to work after migrating from the EMS 13.2.3 to the RAMP 24.06. | <p><b>Impact Statement:</b> The PM Administration-related values were not migrated.</p> <p><b>Resolution Details:</b> Updated the migration process to include these values during the migration.</p>                                                                                                                                                                                                                                                                                                                                                                                       |

| Issue ID  | Original Issue | Sev | Problem Description                                                                                       | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------|----------------|-----|-----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-11713 | N/A            | 2   | The EMS alarm's <code>varbind</code> order differs from the order defined in the MIB.                     | <p><b>Impact Statement:</b> The <code>varbind</code> order mismatch leads to the NBI issue.</p> <p><b>Resolution Details:</b> Modified the code to align the <code>varbind</code> order correctly.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| AFM-11771 | N/A            | 2   | Generate the <code>authKey</code> and <code>privKey</code> using the RAMP.                                | <p><b>Impact Statement:</b> The <code>snmpkey</code> package is missing from the RAMP.</p> <p><b>Resolution Details:</b> Added <code>snmpkey</code> package to the RAMP.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| AFM-11778 | N/A            | 2   | Agent - PSX CNe PIPE container restarts on a fresh install.                                               | <p><b>Impact Statement:</b> The PIPE container restarts while registering to the RAMP during orchestration. The PSX was not registered to the RAMP, resulting in a PIPE container restart during the deployment. The cash used to modify the agent password occasionally exited, which led to registration failures. During the PSX registration process with the RAMP, the <code>sonusAgent</code> running on the PSX occasionally failed to log in using the given credentials. The login sequence takes more time (3-15 seconds) due to a network-induced delay. Also, the JVM parameters to set the Initial <code>Heapsize</code> and <code>Max</code>. The outdated <code>Heapsize</code> does not work in Java 8 in the <code>jash</code> script.</p> <p><b>Resolution Details:</b> Modified the code to contain the proper JVM arguments supported in Java 8 in the <code>jash</code> script.</p> |
| AFM-11780 | N/A            | 2   | The LDAP server FQDN resolution fails from the IPv6 RAMP when the LDAP is configured with the dual stack. | <p><b>Impact Statement:</b> The RAMP CNe to LDAP server FQDN resolution fails on IPv6 deployments when the DNS resolution for the LDAP returns both the IPv4 and IPv6 addresses.</p> <p><b>Resolution Details:</b> Modified the code to prefer the IPv6 address in case of IPv6 deployment.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Issue ID  | Original Issue | Sev | Problem Description                                                                  | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------|----------------|-----|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-11869 | N/A            | 2   | The PM YAML files for the DSC need a refresh/update.                                 | <b>Impact Statement:</b> The DSC Linkset statistics were empty after an upgrade from DSC 22.0 to 23.0.<br><b>Resolution Details:</b> Added a few new attributes to the Linkset statistics related to Unit Data Service (UDTS) and Extended Unit Data Service (XUDTS). Added new YAML for the DSC version 23.0 that includes the new attributes.                                                                                                      |
| AFM-11871 | N/A            | 2   | The EdgeMarc PCAP Diagnostic Snapshot fails to work in the public IP setup.          | <b>Impact Statement:</b> The RAMP with a public IP different from the private IP, the PCAP, and the diagnostic snapshot were not consumed by the device.<br><b>Resolution Details:</b> Updated the EV service code to send public IP to the device where the device can send PCAP and diagnostic snapshot information.                                                                                                                               |
| AFM-11891 | N/A            | 2   | Authorize the Configure action only through the Configuration Management Permission. | <b>Impact Statement:</b> The RAMP permits the Configure action only if the Device Administration permission is enabled. There is no option to enable only the Configure action without allowing the other actions for the node, such as Register, Discover, Edit, Unregister, and Delete.<br><b>Resolution Details:</b> Modified the code to enable the Configure action if the user holds the operator permission for the Configuration Management. |

| Issue ID  | Original Issue | Sev | Problem Description                                 | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------|----------------|-----|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-11939 | N/A            | 2   | Object store does not stabilize on the VMware RAMP. | <p><b>Impact Statement:</b> This issue is not reproducible on all the RAMP VMware installations. The <code>entropy_avail</code> value in the specific RAMP VMware installation was relatively low, causing the random number generation failure in the object store service, which led to a stagnant state.</p> <p><b>Resolution Details:</b> Object store service thread was stuck due to low entropy when using the <code>SecureRandom.getInstanceStrong</code> method. Modified the code to remove this.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| AFM-11940 | N/A            | 3   | Document the new script added for AFM-11823.        | <p><b>Impact Statement:</b> Update the Administration Guide since allowing the algorithm HMACSHA1 is incorporated with a few other cryptographic algorithms in a new script, <code>updateSystemCryptoPolicy.sh</code>.</p> <p><b>Resolution Details:</b> Updated the following documents:</p> <ul style="list-style-type: none"> <li>• <a href="#">Legacy Device Management</a>: Created this page with a procedure to support managing legacy devices, Federal Information Processing Standards (FIPS) are disabled.</li> <li>• <a href="#">Migrate Insight EMS to RAMP</a>: For users having the GSX, after an upgrade and migration, before discovering GSX, run the script:<br/> <pre>/opt/sonus/ems/conf/ updateSystemCryptoPolicy .sh</pre> For more information, refer to <a href="#">Legacy Device Management</a>.</li> <li>• <a href="#">Post-Upgrade Procedures for RAMP</a>: After a RAMP upgrade, to discover the GSX, refer to <a href="#">Legacy Device Management</a>.</li> </ul> |

| Issue ID  | Original Issue | Sev | Problem Description                                                                                       | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------|----------------|-----|-----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12006 | N/A            | 2   | A few of the SBC nodes take longer than expected to display online on the RAMP.                           | <p><b>Impact Statement:</b> If more than one SBC discovery is in progress, it takes a long time for all of them to complete and for the nodes to go online. The REST client connection pool in the Device Manager only allows two connections per route. Many requests go internally to other microservices and use the same route through Apache. One of these requests did not release the connection, which led to blocking other requests waiting for a thread.</p> <p><b>Resolution Details:</b> Added the missing "close" action to ensure the thread gets released. Also increased the number allowed connections per route to account for the number of requests that use Apache.</p>                                                                      |
| AFM-12042 | N/A            | 2   | The RAMP fails to establish the connection when launching the PSX Manager since the RAMP FIPS is enabled. | <p><b>Impact Statement:</b> The RAMP fails to provision the PSX.</p> <p><b>Resolution Details:</b> Modified the code to launch the PSX manager with FIPS enabled.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| AFM-12070 | N/A            | 2   | The Retry Mechanism for the SBC<br><code>setConfigStore</code> to handle the failure case.                | <p><b>Impact Statement:</b> At the end of a dynamic SBC node discovery, the <code>config store</code> parameter is set to enable the SBC to upload the configurations to the RAMP. If this fails, the configuration upload fails without indication, and there is no upload reattempt. A network interruption or other cause that allows a subsequent attempt to succeed can lead to this failure.</p> <p><b>Resolution Details:</b> Added the <code>config store</code> parameter setting to the discovery retry mechanism to ensure if the upload fails, another discovery attempt is made. If the upload fails, but the maximum number of discovery retry attempts is reached, the failure reason indicates that the config store parameter setting failed.</p> |

| Issue ID  | Original Issue | Sev | Problem Description                                                            | Resolution                                                                                                                                                                                                                                                                                                                                            |
|-----------|----------------|-----|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12130 | N/A            | 2   | Gaps with RAMP SFTP pull of GSX PM statistics files in the GSX streaming Mode. | <b>Impact Statement:</b> The SFTP collection fails if the DSI NFS is not mounted.<br><b>Resolution Details:</b> Added SFTP support to the GSX PM statistics in the streaming mode, so mounting the NFS is no longer necessary.                                                                                                                        |
| AFM-12136 | N/A            | 2   | All GSXs indicate "registered offline" due to token expirations.               | <b>Impact Statement:</b> All GSXs indicate "registered offline" with a stale-session/expired token after the user issues a "discover-all" command.<br><b>Resolution Details:</b> Modified the code to log the user out on a session timeout.                                                                                                          |
| AFM-12160 | N/A            | 2   | The SBC SWe Edge firmware upgrade using the RAMP fails.                        | <b>Impact Statement:</b> The SBC SWe Edge firmware upgrade using the RAMP fails when the image contains the string ".build".<br><b>Resolution Details:</b> Modified the code to allow ".build" in the 1k/2k build filenames.                                                                                                                          |
| AFM-12161 | N/A            | 2   | (RAMP CNF) RAMP SSH access support using Active Directory.                     | <b>Impact Statement:</b> The Samba packages were missing from the RAMP after migrating from the EMS.<br><b>Resolution Details:</b> Added the following libraries: <ul style="list-style-type: none"><li>• samba</li><li>• samba-common</li><li>• samba-winbind</li><li>• samba-client</li><li>• samba-winbind-clients</li><li>• authconfig.</li></ul> |



| Issue ID  | Original Issue | Sev | Problem Description                                 | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|----------------|-----|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12203 | N/A            | 2   | The PM collection issue exists on the SGX 10.0.6R0. | <p><b>Impact Statement:</b> For SGX version 10.0.6R0, the memory usage-related counters in the PM statistics are not pegged or pegged as "0." This is a known issue in the SGX 10.0.6R0 release, and the fix is available for a higher release. Ribbon previously provided a script in the EMS to run as a cron job to collect memory information from the SGX. This is also needed in the RAMP CNF for the SGX 10.0.6R0 to retrieve memory information.</p> <p><b>Resolution Details:</b> The script <code>/opt/sonus/ems/conf/sgx-mem-collector.sh</code> is added in the RAMP CNF to run as an Insight cron job every 15 minutes in RAMP by default.</p> |
| AFM-12244 | N/A            | 2   | Missing support for the old versions of PSX APIs.   | <p><b>Impact Statement:</b> The user holds the PSX version 14.1.3 and provisions through the RAMP API with the PSX WSDL version r07_03_02.</p> <p><b>Resolution Details:</b> The RAMP is enhanced to support the older versions of PSX APIs (from 7.0.x to 8.2.x).</p>                                                                                                                                                                                                                                                                                                                                                                                      |
| AFM-12244 | N/A            | 2   | Support the old PSX API version.                    | <p><b>Impact Statement:</b> The support for 07_00_00 and above versions were missing in the RAMP.</p> <p><b>Resolution Details:</b> Added the support from 07_00 to 08_02_00 in the RAMP.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| AFM-12296 | N/A            | 2   | The RAMP fails to launch the SBC Manager GUI.       | <p><b>Impact Statement:</b> The RAMP fails to launch the SBC Manager GUI when the .KF file is generated using the DES algorithm since the SBC Manager in the RAMP does not support the DES algorithm.</p> <p><b>Resolution Details:</b> Support for the DES algorithm was added in the SBC Manager.</p>                                                                                                                                                                                                                                                                                                                                                     |

| Issue ID  | Original Issue    | Sev | Problem Description                                                                                       | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------|-------------------|-----|-----------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12361 | N/A               | 2   | Error logs are generated in the <code>ems_trace_log</code> when the PSX API provisioning is accomplished. | <p><b>Impact Statement:</b> When the Application Config -&gt; Utils -&gt; Enable CLI/API username logging is set to True, an exception is observed in the logs, and the connection is not freed. When the flag is set to True, the <code>nodeId</code> is passed into <code>freeConnection</code> as "<code>nodeId+userName</code>," causing an exception when trying to retrieve the provisioning PSX.</p> <p><b>Resolution Details:</b> Added a <code>freeConnection</code> to match the <code>getConnection</code> and handle the extra username parameter.</p>                                                                              |
| AFM-12369 | N/A               | 2   | SBC CNe: The SBC Manager GUI connection through the RAMP window relaunches.                               | <p><b>Impact Statement:</b> The SBC GUI running on the RAMP frequently runs a REST call to the SBC on port 443 to check if the SBC is up and running. Occasionally, the REST call fails with an error "Connection reset by peer (connect failed)", leading the SBC GUI to consider that the SBC is down, and the GUI relaunches with only limited functionality. After an interval, the REST call succeeds, and the GUI is relaunched with complete functionality.</p> <p><b>Resolution Details:</b> Implemented the retry mechanism to address the failure while connecting to the device before reporting failure to the SBC Manager GUI.</p> |
| AFM-12399 | AFM-12456 (24.06) | 2   | Allow MAC and KEX algorithms on the RAMP 8122 CLI.                                                        | <p><b>Impact Statement:</b> A few deprecated MAC and KEX algorithms were removed as part of security updates. However, these algorithms are required while connecting to older devices using the RAMP CLI.</p> <p><b>Resolution Details:</b> The RAMP is enhanced to read the MAC and KEX algorithms from <code>/opt/sonus/ems/weblogic/sonusEms/data/cli/framework/resources/Listener.properties</code> file.</p>                                                                                                                                                                                                                              |

| Issue ID  | Original Issue | Sev | Problem Description                                                                                              | Resolution                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------|----------------|-----|------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12407 | N/A            | 2   | The RAMP fails to export the <code>DspResDspUsageIntervalStats</code> to the IT systems due to an SBC7K upgrade. | <p><b>Impact Statement:</b> The SBC7K device fails to process <code>DspResDspUsageIntervalStats</code>. The <code>mdjson</code> file used by the PM Persister component is missing a few expected fields for SBC 11.2.x devices.</p> <p><b>Resolution Details:</b> This issue is resolved in the previous version of the RAMP and verified in RAMP 24.09.</p>                                                                                                                                                                 |
| PLTF-4305 | N/A            | 2   | Deprecated SSH cryptographic ciphers.                                                                            | <p><b>Impact Statement:</b> The SSH cipher vulnerabilities are reported in the Qualys scan. When the Crypto policy is set to DEFAULT/FIPS, the deprecated ciphers are enabled in those configuration files, and vulnerabilities are reported.</p> <p><b>Resolution Details:</b> Added strict MACs and Ciphers on the RHEL7 in both the <code>/etc/ssh/ssh_config</code> and <code>/etc/ssh/sshd_config</code> files.</p>                                                                                                      |
| PLTF-4478 | N/A            | 2   | RAMP 24.06: etcd upgrade support.                                                                                | <p><b>Impact Statement:</b> The etcd upgrade-related documentation is not available.</p> <p><b>Resolution Details:</b> Created the documents for different upgrade configurations. For more information, refer to:</p> <ul style="list-style-type: none"> <li>• <a href="#">Upgrading etcd</a></li> <li>• <a href="#">Upgrading etcd on KVM</a></li> <li>• <a href="#">Upgrading etcd on VMware</a></li> <li>• <a href="#">Upgrading etcd on Openstack</a></li> <li>• <a href="#">Upgrading etcd on Kubernetes</a></li> </ul> |

## Known Issues

### Severity 1 Issues

There are no severity 1 known issues in this release.

### Severity 2 and 3 Issues

The following table lists the severity 2 and 3 known issues in this release:

| Issue ID | Sev | Problem Description                                                                                                                                                               | Impact/Workaround                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-4461 | 2   | When the active RAMP goes down in an Active/Active scenario, the Standby registers a "relocate" action while the Active becomes active again, resulting in loss of functionality. | <b>Impact Statement:</b> The RAMP server goes down, and manual intervention is required to bring it up.<br><b>Workaround:</b> N/A                                                                                                                                                                                                                                                                                                                                                                                             |
| AFM-6966 | 2   | Retain all the passwords after a restore (Upgrade/Migration).                                                                                                                     | <b>Impact Statement:</b><br><ol style="list-style-type: none"><li>1. Linux Insight user (insight) - Reset post restore</li><li>2. Linux Admin user (admin) - Reset post restore</li><li>3. Insight DB user - Retained</li><li>4. Insight Postgres DB user - Reset</li><li>5. Insight Agent (admin) - Retained</li><li>6. Insight GUI Admin user (admin) - Reset</li><li>7. Insight REST API user (restuser) - Retained</li><li>8. Insight GUI Admin User (admin) - Reset</li></ol> <b>Workaround:</b> Set the password again. |
| AFM-7086 | 3   | Localhost Auto discovery failed (CNF).                                                                                                                                            | <b>Impact Statement:</b> The Localhost registration failed. The PM and other functionalities are impacted.<br><b>Workaround:</b> Navigate to the DM page and manually re-discover the local host.                                                                                                                                                                                                                                                                                                                             |
| AFM-7320 | 3   | The SBC CNe nodes are not registered in the extended IPv6 format.                                                                                                                 | <b>Impact Statement:</b> No functionality impact. IPv6 addresses display in short form.<br><b>Workaround:</b> N/A                                                                                                                                                                                                                                                                                                                                                                                                             |

| Issue ID | Sev | Problem Description                                                                                                           | Impact/Workaround                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|-----|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-7578 | 3   | The node service must stop if the reachability consumer stops due to an exception.                                            | <p><b>Impact Statement:</b> The node management application starts even if the KAFKA consumer reachability stops due to an unexpected error, which results in an inconsistent system state.</p> <p><b>Workaround:</b> If the node status is not updated according to the reachability polling results, follow these instructions to restart the dynamic node services.</p> <ol style="list-style-type: none"> <li>1. Log on as an insight user.</li> <li>2. Run the following commands: <pre>cd /opt/devMgmt/bin ./dynamicNodeService stop ./dynamicNodeService start</pre> </li> </ol> |
| AFM-7891 | 3   | The SBC SWe Edge configuration fails on the RAMP.                                                                             | <p><b>Impact Statement:</b> The RAMP fails to launch the SBC GUI configuration on the SBC SWe Edge. This is a rare occurrence attributed to a tunnel creation failure.</p> <p><b>Workaround:</b> Reboot the SBC SWe Edge instance.</p>                                                                                                                                                                                                                                                                                                                                                  |
| AFM-8483 | 2   | The <code>PeerIPAddress</code> field contains the worker node IP address instead of the RAMP IP address in the SNMP receiver. | <p><b>Impact Statement:</b> The <code>PeerIPAddress</code> field contains the worker node IP address and port. The <code>PeerIPAddress</code> field must contain RAMP's eth1 IP address instead of the worker node IP address because the worker node IP address changes when the pod is moved from one worker node to another.</p> <p><b>Workaround:</b> N/A</p>                                                                                                                                                                                                                       |
| AFM-8777 | 3   | The SBC registration fails with <code>emsIpAddressOverride</code> .                                                           | <p><b>Impact Statement:</b> The SBC registration fails with <code>emsIpAddressOverride</code> if the RAMP IP address is changed.</p> <p><b>Workaround:</b> Remove the Node ID from the SBC User Data and resend the Registration Request.</p>                                                                                                                                                                                                                                                                                                                                           |

| Issue ID  | Sev | Problem Description                                                                                                                                                              | Impact/Workaround                                                                                                                                                                                                                                                                                              |
|-----------|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-9595  | 3   | Legacy devices such as GSX PM metrics are not available in the Prometheus if the number of devices is greater than 15.                                                           | <p><b>Impact Statement:</b> The RAMP CNF observability performance issues limit the capacity of the observability component to process the GSX metrics.</p> <p><b>Workaround:</b> Export the PM data to an external server.</p> <p>Note: Maximum of 10,000 metrics are exported to Prometheus.</p>             |
| AFM-9658  | 3   | Missing clearing event <code>sonusHARACProcessUPNotification</code> for problem event <code>sonusHARACProcessDownNotification</code> for FM processes restarted by the openSAF.  | <p><b>Impact Statement:</b> The clearing event does not occur through the FM process.</p> <p><b>Workaround:</b> Run the <code>emsMgmt</code> command to verify the state of the FM process.</p>                                                                                                                |
| AFM-10033 | 3   | The RAMP fails to fetch the complete <code>oam</code> , <code>snmp</code> , <code>trapTarget</code> using the CLI in IPv6.                                                       | <p><b>Impact Statement:</b> The RAMP CLI issue occurs when the RAMP fails to display the complete response if the response size exceeds 80 characters for the particular column. The window size is truncated whenever it reaches 80 characters. This applies to all tables.</p> <p><b>Workaround:</b> N/A</p> |
| AFM-11210 | 3   | Performance Load: When all the nodes go offline, the RAMP takes time to bring up all the nodes online as reachability timeout is high, which results in waiting for the threads. | <p><b>Impact Statement:</b> When a huge number of nodes goes offline, the RAMP takes time to bring all the nodes back online.</p> <p><b>Workaround:</b> N/A</p>                                                                                                                                                |
| AFM-11222 | 3   | Multi-Tenancy: Limit the Resource Group access within the tenant hierarchy.                                                                                                      | <p><b>Impact Statement:</b> The user can edit/delete the resource group above the tenant hierarchy.</p> <p><b>Workaround:</b> N/A</p>                                                                                                                                                                          |

| Issue ID  | Sev | Problem Description                                                                                                                 | Impact/Workaround                                                                                                                                                                                                                                                                                                                                   |
|-----------|-----|-------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-11239 | 3   | The RAMP CNe fails to perform the Restore Revision because it cannot download the complete configuration file (Random occurrences). | <p><b>Impact Statement:</b> The RAMP fails to perform Restore Revision because it fails to download the complete configuration file. Manually downloading the configuration file fails partially.</p> <p><b>Workaround:</b> Restart the SBC.</p>                                                                                                    |
| AFM-11349 | 3   | The Cluster Management table does not navigate to the previous page after deleting a cluster from the last page (RAMP GUI).         | <p><b>Impact Statement:</b> The user cannot view the existing clusters. However, the table is loaded if clicked again. This problem is observed only if the cluster is deleted from the last page, not from the first page or an intermediate page.</p> <p><b>Workaround:</b> Visit the Cluster Management page and return to the current page.</p> |
| AFM-11718 | 3   | TrunkGroupDataExporter reports are incomplete and slow.                                                                             | <p><b>Impact Statement:</b> The TG reports for ALL GSX are slow. For each GSX, it takes approximately three hours to receive the TG data for the TrunkGroup CSV.</p> <p><b>Workaround:</b> N/A</p>                                                                                                                                                  |
| AFM-12061 | 2   | The EMS CLI Port 8122 drops the first character.                                                                                    | <p><b>Impact Statement:</b> When performing a copy/paste of multiple CLI commands in the RAMP CLI port 8122 (SSH), the first command runs correctly, but the subsequent commands fail because the first character is dropped.</p> <p><b>Workaround:</b> Add an empty line between each command and then run the script.</p>                         |
| AFM-12063 | 3   | 24.09 (FM): Unable to load the FM Administration page (Single occurrence).                                                          | <p><b>Impact Statement:</b> Due to an FM administration page issue, the FM REST Service generates the error "Error Loading Administration Page."</p> <p><b>Workaround:</b> Restart the FM REST Service.</p>                                                                                                                                         |

| Issue ID                 | Sev | Problem Description                                                                                 | Impact/Workaround                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|-----|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-12357                | 3   | The RAMP switchover is not triggered when the OpenSAF is down (Negative scenario).                  | <b>Impact Statement:</b> The RAMP fails to perform a Switchover in the GR (Rare negative scenario).<br><b>Workaround:</b> Trigger the switchover manually.                                                                                                                                                                                                 |
| AFM-12449                | 3   | Email address support for the RAMP GUI certificate.                                                 | <b>Impact Statement:</b> Missing email address when creating a CSR for the RAMP GUI.<br><b>Workaround:</b> N/A                                                                                                                                                                                                                                             |
| AFM-12482/<br>CHOR-12687 | 3   | The RAMP fails to launch the SBC SWe Edge configuration page after an upgrade.                      | <b>Impact Statement:</b> Unable to launch the SBC SWe Edge device page on the upgraded RAMP server.<br><b>Workaround:</b> Reboot the SBC SWe Edge device.                                                                                                                                                                                                  |
| AFM-13080                | 2   | The RAMP fails to migrate the Mediation Server for the Lawful Interface.                            | <b>Impact Statement:</b> The Mediation Server configuration are not carried to the RAMP during the EMS to RAMP migration.<br><b>Workaround:</b> Re-configure the Mediation Server after an EMS to RAMP migration.                                                                                                                                          |
| AFM-13100                | 3   | RAMP CNF: Handling the timestamp format (ISO8601 format) correctly in the RAMP logs.                | <b>Impact Statement:</b> Enhancement to handle the timestamp format (ISO8601 format) correctly in the RAMP logs.<br><b>Workaround:</b> N/A                                                                                                                                                                                                                 |
| AFM-13112                | 2   | The CliFramework fails to create a connection to the SBC if the username does not end with "admin". | <b>Impact Statement:</b> Unable to process the CLI command for the SBC.<br><b>Workaround:</b> <ol style="list-style-type: none"><li>1. Create a user in the SBC with a name ending with 'admin'. For example, emsdiscoveryadmin.</li><li>2. Register an SBC with this newly created NETCONF user to ensure the CLI functionality runs correctly.</li></ol> |



| Issue ID  | Sev | Problem Description                                                                         | Impact/Workaround                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------|-----|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-13166 | 2   | Address the PM export issues for large loads in single export profile for each device type. | <p><b>Impact Statement:</b> The GSX statistics data is lost when the PM export is enabled with many GSX devices in a single export profile.</p> <p><b>Workaround:</b> Create multiple PM export profiles for the GSXs and assign them equally to the GSX devices.</p> <p><b>Note:</b> Do not configure more than 100 device per export profile when the PM export mode is set to Per Node Export.</p>                                                 |
| AFM-13206 | 2   | Export fails in large networks with the error "Argument list too long" for perNodeExport.   | <p><b>Impact Statement:</b> The perNode export fails in the large network when:</p> <ol style="list-style-type: none"><li>1. A large number of devices are registered in the RAMP (more than 400)</li><li>2. Node Name of the device is too long (more than 20 characters)</li><li>3. All devices are part of one single PM export profile.</li></ol> <p><b>Workaround:</b> Ensure that an export profile does not contain more than 100 devices.</p> |

| Issue ID  | Sev | Problem Description                                                                                   | Impact/Workaround                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|-----|-------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-13210 | 2   | Include re-generating CSR in post-migration steps.                                                    | <p><b>Impact Statement:</b> Discovery fails on the RAMP after a migration.</p> <p><b>Workaround:</b> Added note in <a href="#">Migrate Insight EMS to RAMP</a>. If the user holds a CA-signed agent certificate on the EMS with MD5withRSA signature algorithm, perform the following procedure after migrating from the EMS to the RAMP, before discovering the nodes:</p> <ol style="list-style-type: none"><li>1. Re-generate the CSR. For more information, refer to <a href="#">Generate Certificate Request for Agent</a>.</li><li>2. Re-import the certificate to the agent keystore. For more information, refer to <a href="#">Import Certificates for Agent</a>.</li><li>3. Restart administration service:<pre># sudo su - insight # cd /opt/devMgmt/bin/ # ./administrationService stop;./ administrationService start</pre></li></ol> |
| AFM-13229 | 2   | RAMP 24.12: The Calea user does not hold permission to access the DM UI after a migration.            | <p><b>Impact Statement:</b> By default, the Calea user does not hold permission to access the DM UI after a migration.</p> <p><b>Workaround:</b> The user needs to add the permission manually.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| AFM-13339 | 3   | The RAMP generates Active Directory Configuration issues during the upgrade and non-cloud deployment. | <p><b>Impact Statement:</b> Active Directory configurations are not retained during the upgrade, causing login failures in non-cloud deployment.</p> <p><b>Workaround:</b> Perform <a href="#">Post-Upgrade Procedures for RAMP</a> and <a href="#">Reconfiguring Active Directory</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Issue ID  | Sev | Problem Description                                                                                                                            | Impact/Workaround                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------|-----|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-13365 | 3   | In multiple interfaces configured on the SBC setup, if the primary interface is disabled, the RAMP discovery fails for SBC after a switchover. | <b>Impact Statement:</b> If one of the interfaces is disabled on the SBC that is returned as the first interface by the SBC, the disabled interface is updated as the primary IP address. If there is an SBC switchover, the node does not come online on the RAMP.<br><b>Workaround:</b> Update the Host IP address fields from the UI after every SBC switchover and do not discover the node after that. |

## Known Limitations

The following limitations exist in this release:

1. Dual-stack RAMP deployment is not supported in the RAMP.
2. IPv6 deployment is not supported on the Azure and AWS platforms.
3. RAMP does not support High Availability redundancy.
4. RAMP supports only standalone deployments on the Azure and AWS platforms.
5. AMP does not support the REST API provisioning for SBC versions less than 11.1.
6. UI dashboard and other FM/PM UIs have issue with Multi-tenancy. They are GUI issues and will be address in Release 25.X release.
7. The following items are not restored as part of the RAMP restore operation.
  - a. Platform-related configurations
  - b. Custom Cron jobs configured by users
  - c. Custom scripts or jobs deployed at the Linux level

## New in RAMP 24.12.00R000

### RAMP 24.12.00R000

The Ribbon Application Management Platform (RAMP) includes the following new features in this release:

#### Note

The Beta features refer to software features available for access within the software build but are still under development. Early access is provided to gather feedback from users. The capability may have limited functionality. The availability of the Beta feature in the current RAMP version does not guarantee that the feature will be available in the future. Ribbon may withdraw the Beta features from any future RAMP release without notice.

| JIRA ID  | Feature Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-5686 | <p><b>Bulk Action Notifications (Beta)</b></p> <p>The RAMP is enhanced with a notification microservice. This capability is targeted for the EdgeMarc device. While initiating actions, users can enable notifications for particular actions. When performing an EdgeMarc bulk action, users can specify whether they need to receive notifications for the action status. It is an optional microservice, and the user can manually add the service after the RAMP installation.</p> <p>For more information, refer to:</p> <ul style="list-style-type: none"><li>• <a href="#">Notifications</a></li><li>• <a href="#">Back up EdgeMarc Devices</a></li><li>• <a href="#">Change Password for EdgeMarc Devices</a></li><li>• <a href="#">Restore EdgeMarc Devices</a></li><li>• <a href="#">Run Health Reports on EdgeMarc Devices</a></li><li>• <a href="#">Upgrade Firmware for EdgeMarc Devices</a></li><li>• <a href="#">Reboot EdgeMarc Devices</a></li><li>• <a href="#">Configure Devices on EdgeMarc</a></li></ul> |
| AFM-5784 | <p><b>Framework Update for User Interface Improvements</b></p> <p>The RAMP UI framework has been updated to enhance the performance and support the Web Content Accessibility Guidelines (WCAG) requirements.</p> <p>For more information, refer to:</p> <ul style="list-style-type: none"><li>• <a href="#">Provision SBC Core</a></li><li>• <a href="#">Compare Uploaded Configurations for SBC Core or SLB Devices</a></li><li>• <a href="#">Provision SBC Edge Devices</a></li><li>• <a href="#">Take Backup of SBC Edge Devices</a></li><li>• <a href="#">Take Backup of SBC Core and SLB Devices</a></li><li>• <a href="#">SBC Edge Devices Catalog Management</a></li><li>• <a href="#">SBC Core and SLB Catalog Management</a></li><li>• <a href="#">Customize the Logon Banner</a></li><li>• <a href="#">Exporting Logs to a Remote Syslog Server</a></li><li>• <a href="#">SSH Active Channels</a></li></ul>                                                                                                        |
| AFM-6413 | <p><b>Forward Manually Cleared Alarms to OSS</b></p> <p>The RAMP is enhanced to support manually clearing an alarm and sending a clear alarm message to the northbound system. An action called Clear with Forward is introduced to generate a warning message when the alarm count limit exceeds.</p> <p>For more information, refer to <a href="#">Monitor Alarms</a></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| JIRA ID   | Feature Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-7310  | <b>Resource Group Dashboard (Beta)</b><br>The RAMP is enhanced to display a dashboard view screen to show all resource groups in a card-style format. You can filter the resource group cards based on criteria.<br>For more information, refer to: <ul style="list-style-type: none"><li>• <a href="#">Dashboard</a></li><li>• <a href="#">Resource Group Dashboard</a></li></ul>                                                                                                                                                                                                                                                                                                                                                               |
| AFM-9216  | <b>Global Search (Beta)</b><br>The RAMP is enhanced by providing a Global Search Service (GSS) to search components and devices available on the RAMP GUI. This functionality is available after manually installing an optional microservice GSS using the script <code>global_search_service_config</code> after installing the RAMP. When this microservice runs, the RAMP publishes a confirmation message over the Kafka topic, <code>service.availability_status</code> . The other microservices consume the Kafka message and then register themselves with the GSS by sending the register request, enabling access to the GSS to display the search results.<br>For more information, refer to <a href="#">Global Search Service</a> . |
| AFM-10192 | <b>Test Migration from EMS 14.1 to RAMP with HP Primary PSX 14.0</b><br>The RAMP 24.12R0 supports the discovery and registration of the HP Primary PSX 14.0 on the RAMP, including the HP Primary PSX 14.0 alarms, logs, statistics, and Performance Management reports.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| AFM-10364 | <b>RAMP Support for ESXi 8.0</b><br>The RAMP supports VMware ESXi 8.0.<br>For more information, refer to <a href="#">System Requirements</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| AFM-10788 | <b>RAMP Default Certificates Update/Renew Before the Expiry Date</b><br>Beginning with the 24.12 release, the RAMP provides scripts that allow the operator to renew existing certificates or create new ones. For the RAMP versions less than RAMP 24.12, you can either renew the existing certificates or create new certificates using the scripts <code>generateCerts.sh</code> and <code>updateRDCerts.sh</code> . These scripts are available in the <code>rampbootstrap.tar</code> file.<br>For more information, refer to <a href="#">Renew RAMP Certificates</a> .                                                                                                                                                                     |

| JIRA ID   | Feature Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AFM-11244 | <p><b>SBC 12.1.4/PSX 16.1.4 Device Support</b></p> <p>The RAMP 24.12 supports the SBC 12.1.4 and PSX 16.1.4 features. An attribute is included in the PSX statistics <b>PsxHTTPCounterStats</b> to display the count of calls for which multiple STI services are run. For more information, refer to <a href="#">PSX Statistics</a>.</p> <p>After manually registering a PSX device on the RAMP, you can modify the Primary to Replica or vice-versa. For more information, refer to <a href="#">Register a PSX Device</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| AFM-12348 | <p><b>PM Enhancements</b></p> <p>The RAMP includes multiple enhancements to the Performance Management service. The ability to disable the running of the JMX and SNMP PM statistics collector process. On a network with devices supporting only SFTP-based collection, operators are allowed to disable these collector processes to improve the RAMP system resource usage. For more information, refer to <a href="#">Configure Performance Management Collection Options</a>.</p> <p>The columns <b>Column Type</b> and <b>Aggregation Type</b> are updated with new entries in the following PSX statistics table on the RAMP:</p> <ul style="list-style-type: none"><li>• <b>SoftSwitchLwresdServerStats</b> - Updated with 23 new column types.</li><li>• <b>SoftSwitchLwresdZoneStats</b> - Updated with 22 new column types.</li><li>• <b>PsxHpcGetsServerStats</b> - Updated with 10 new column types.</li><li>• <b>PsxHpcGetsZoneStats</b> - Updated with 10 new column types.</li></ul> <p>For more information, refer to:</p> <ul style="list-style-type: none"><li>• <a href="#">PSX Statistics</a></li><li>• <a href="#">Configure Performance Management Collection Options</a></li></ul> |