NN10369-111

Succession

Carrier Voice over IP

Management Module Basics

(I)SN07 Standard 02.02 December 2004

NORTEL NETWORKS™

Overview

The Management Module is a key component of the Preside Management for Succession Solutions (Preside MSS). It supports the services used to communicate with and manage the RTP Media Portal, Oracle Monitor, and Database Modules and their hosting servers. In addition, the Management Module interacts with the System Management Console used by administrators as the element manager.

Topics in this chapter

How this guide is organized

This guide contains the following information:

- Upgrades

  Describes the upgrade strategy of the Management Module software.

- Fault management

  Describes the fault management strategy and manual fail over of the Management Module.

- Configuration management

  Describes the configuration strategy and the property fields of the Management Module component services.

- Accounting

  Describes the accounting activities of the Management Module.

- Performance management

Describes the performance management strategy of the Management Module software and hosting servers.

- Security and administration

  Describes the security issues and administrative tasks related to the operations of Management Module services.

Management Module functions and services

The Management Module component provides the services that support the communication between the system components and System Management Console. In conjunction with the System Management Console, the Management Module supports the following functionality:

- system operations administration
- system software management
  - software inventory
  - software updates
  - deployment, launch, and monitoring
- system configuration
  - query, add, modify, delete
- system maintenance
  - lock and unlock services
  - firmware upgrades
- fault monitoring
  - logs
  - alarms
  - archival of logs (which includes fault events)
- system performance monitoring
  - counters and meters
  - configurable collection period and archival of performance measurements
- network management interfaces
  - Extended Markup Language over Transmission Control Protocol (XML/TCP), Perfect Channel Protocol (PCP)
  - System Management Console

Management Module interfaces

In the CVoIP system communications scheme, the Management Module sits between the system components and the System Management Console.

The following are the interfaces of the Management Module:

- Transmission Control Protocol (TCP) interface
- Structured query language (SQL) interface
- Simple network management protocol version 2 (SNMPv2) interface
- Secure File Transfer Protocol (SFTP) interface

Transmission Control Protocol (TCP)

The Management Module uses TCP to communicate management and configuration data to each of the managed network elements. Likewise, the managed network elements use TCP to communicate performance data, logs, and alarms upwards to the Management Module

Structured query language (SQL)

SQL (over a Java Database Connection – JDBC) is used for storing and retrieving system configuration data between the Management Module and the Database Module(s).

Simple Network Management Protocol version 2c (SNMPv2c)

SNMPv2c is used to poll the Management Module for alarm events. The SNMPv2c polling can be used to report alarms to an existing network management system.

Secure File Transfer Protocol (SFTP)

SFTP is used to transfer data from the Management Module to a northbound management system for logs, operational measurements (OMs).

Management Module hosting hardware

A Sun Netra 240, Sun Fire V240, or Sun Fire V100 server(s) hosts the Management Module component(s). The following table gives a highlevel description of the hardware details of the hosting servers.

Table 1 Management Module hosting hardware

Hardware	Details
Sun Fire V240 or Sun Netra 240  Although essentially the same, the Sun Fire V240 is AC powered, whereas the Sun Netra 240 is DC powered.	Both the Sun Fire and Netra 240 servers have the following hardware features: • 2 x 1.2 GHz UltraSPARC IIIi processors • 4 GB RAM • 1MB Internal Cache • 2 x 73GB hard disks • 1 x internal DVD-ROM Drive • 4 x 10/100/1000 Base-T Ethernet Ports • 2 x USB Ports • 2 x Serial Ports
Sun Fire V100 	The server has the following hardware features: • 1 x 650 MHz UltraSparc IIi processor • 1 GB RAM • 512 Kb on-chip L2 cache • 2 x 40 GB hard disks • 2 x 24x internal CD-ROM • 2 x 10/100 Base-T Ethernet ports • 2 x USB ports • 2 x Serial ports

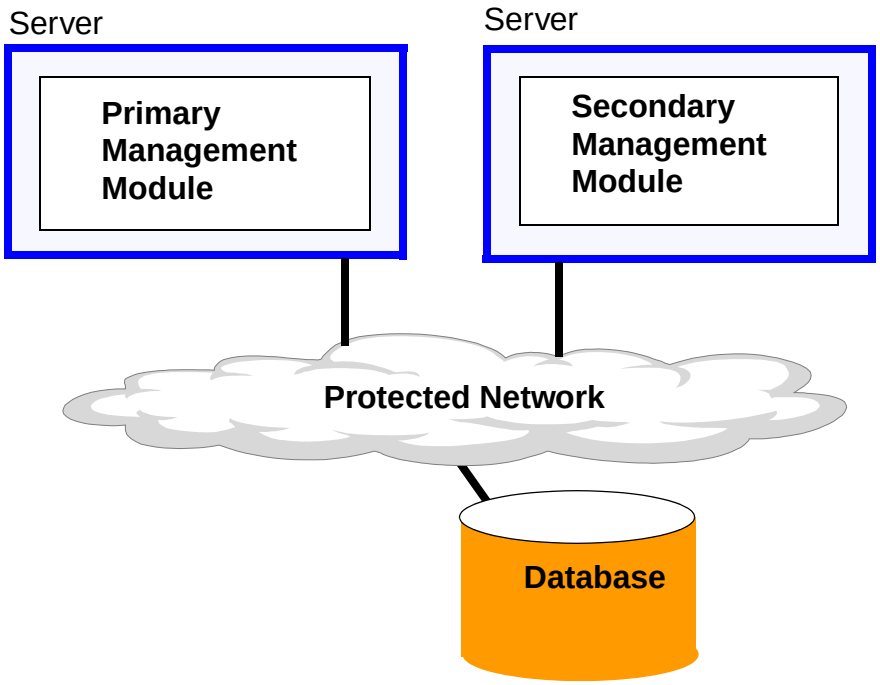
Fault tolerance (optional)

In a standard deployment, their is one instance of the Management Module hosted on a shared server. The redundant network architecture is optional.

In redundant network architectures, the Management Module is hosted on two servers. One server hosts the primary Management Module. A second server hosts the secondary Management Module. If the primary

Management Module or its hosting server fails, a manual failover allows the transfer of the Management Module operations to the secondary module. A logical view of the setup is shown in the following figure.

Figure 1 Management Module redundancy option - logical view



The database stores the system application and configuration data. The secondary Management Module retrieves the latest configuration data from the database when it becomes active. However, all information stored on the management server's local disk is not transferred during a manual failover. This information includes archived logs and holding operational measurements (OMs).

Upgrades

Topics in this chapter

Upgrade and update strategy and tools

Full upgrades to the Management Module software should only be performed with involvement from your next level of support.

For updates, system administrators use a script that automates the manual deployment of a new Management Module version, and the undeployment of the existing version. The script must be executed as a Nortel Networks or root user. In most instances, this requires the involvement of your next level of support.

When there is a primary (active) and cold standby Management Module, the standby can be updated without interruption of Management Module services or the loss of the System Management Console connection. When updating the primary Module, the Management Module processes are stopped and Management Console connection is lost.

For more information, see the procedure Updating the Management Module.

Updating the Management Module

Updating the Management Module version is performed using a script. The script is run on the server hosting the Management Module and requires root or Nortel Networks server access privileges. This may require involvement from your next level of support.

System administrators require the following information when performing the procedure and running the software update script.

- Physical IP address of the server hosting the Management Module being updated
- Management Module software version (load name)
- Whether or not the database is replicated
- Primary database logical IP address
- Secondary database logical IP address if the database is replicated
- Management Module logical IP address
- Whether or not a Motorola SAM 16 Media Server (SIP PRI gateway or SIP audio server) will be deployed

from the administrator workstation

1 Log onto the server hosting the Management Module being updated using the physical IP address of the server.

2 Run the Management Module deploy script.

`/opt/sb/dsm2/bin/mgmtdeploy.pl`

A list of the available versions (loads) will be listed. The following is an example of a load list display:

```
[1] mgmtsvr_all-micro_ims_3.0.4_build306
[2] mgmtsvr_all_small_ims_3.0.4_build306
[3] mgmtsvr_all_ims_3.0.4_build306
[4] mgmtsvr_all-micro_ims_3.0.4_build324
[5] mgmtsvr_all-small_ims_3.0.4_build324
[6] mgmtsvr_all_ims_3.0.4_build324
```

3 The script prompts the system administrator for required configuration information. The script uses the current

configuration information to fill in the prompt defaults displayed in the closed brackets [ ].

Please enter the number of the load to deploy:

Enter the number of the Management Module version from the displayed list.

Is the Database Replicated? [Y]:

Enter either Y or N.

Enter Machine Logical IP Address - Primary DB [current_ip_address]:

Enter the logical IP address of the primary database. By default, the script uses the IP address from the current configuration.

Enter Machine Logical IP Address - Secondary DB [current_ip_address]:

If the database is replicated, enter the logical IP address of the secondary database. By default, the script uses the IP address from the current configuration.

Enter Machine Logical IP Address - MgmtSvr [current_ip_address]:

Enter the logical IP address of the Management Module. By default, the script uses the IP address from the current configuration.

Will a Motorola SAM 16 Media Server (SIP PriGwy or SIP Audio Svr) be deployed? [Y]:

Enter either Y or N.

4 Once the configuration information is entered, the script lists the entered values.

```
Information obtained for Mgmtsvr
deployment/configuration:

mgmtsvr load name = <Management_Module_load>

Database Replicated = <Y_N>

Machine Logical IP Address - Primary DB =
<logical_ip_address>

Machine Logical IP Address - Secondary DB =
<logical_ip_address_if_DB_replicated>

Machine Logical IP Address - Mgmtsvr =
<logical_ip_address>
```

```
Motorola SAM 16 Media Server (SIP PriGwy or SIP
Audio Svr) deployed = <Y_N>
```

The script prompts the system administrator to confirm the configuration information.

`Is the above data correct? [Y]:`

5 The system checks for existing loads. The script prompts the user to undeploy the current Management Module version.

`Do you want the <existing_load_name> load undeployed? [Y]:`

Enter Y to undeploy the current version. When Y is entered, the current load will be undeployed before the new load is deployed.

Various progress and log information messages are sent to the workstation during the undeployment and deployment.

6 The scripts prompts the administrator to define the state of the updated Management Module.

`Startup the SysMgr and TSS processes? [Y]:`

Where,
Y = component becomes active, brings up Svc IP and SysMgr processes
N = component remains in standby mode, without processes running

The Management Module update is finished, and the following message is displayed:

```
/usr/bin/perl -I/opt/sb/dsm2/bin/ /opt/sb/dsm2
/bin/mgmtsvrUtility.pl /opt/sb/dsm2/bin was
successful
```

7 Log off the server.

The updated Management Module will be in the state as defined in the step 6.

Fault management

Topics in this chapter

Fault management strategy and tools

The primary fault management information used by administrators are alarms and logs. The Management Module services collect and archive the alarms and logs generated by the system devices and components. Once collected, administrators can view the fault information using the System Management Console.

The following System Management Console tools are used for viewing and working with alarms and logs collected by Management Module:

- General information area (GIA)

  Administrators use the GIA of the System Management Console to view high level operational information and alarm totals for the Management Module and its hosting server.

- Alarm browser

Administrators use the alarm browser to view alarms generated by the services of the Management Module.

- Log browsers

  Administrators use the current and archive log browsers to view and save operational event information related to the services of the Management Module. Either a system or a manual action can generate a log. Logs include status and activity reports, hardware or software alarms, changes in state, and other events or conditions affecting the Management Module and all other managed network elements.

For information on using the System Management Console tools, refer to the *CVoIP System Management Console User Guide*.

If a fault results in the primary Management Module or its hosting server going down in a redundant configuration, administrators can perform a manual failover to activate the secondary Management Module from its cold standby state.

Hosting server backup and restore

There are capabilities to back up and recover CVoIP server software and hardware as a result of specific hardware failures. These capabilities range from the ability to recover the hardware and software after minor server failures to the recovery of hardware and software after catastrophic server failures.

Backups of Management Module's hosting server(s) is recommended in order to recover from a catastrophic failure where a complete restore of the server's software (both third party and component software) and server configuration information is required.

ATTENTION

Backups of CVoIP hosting servers are highly recommended in certain situations based on the software resident on the server. These situations include when the Solaris Operating System on any CVoIP server is updated, and when an CVoIP software maintenance release for the Management Module is deployed to a server.

Lost System Management Console connection

When the connection between the Management Module and System Management Console is lost, the following dialog box appears on the administrator's workstation screen followed by a login prompt.

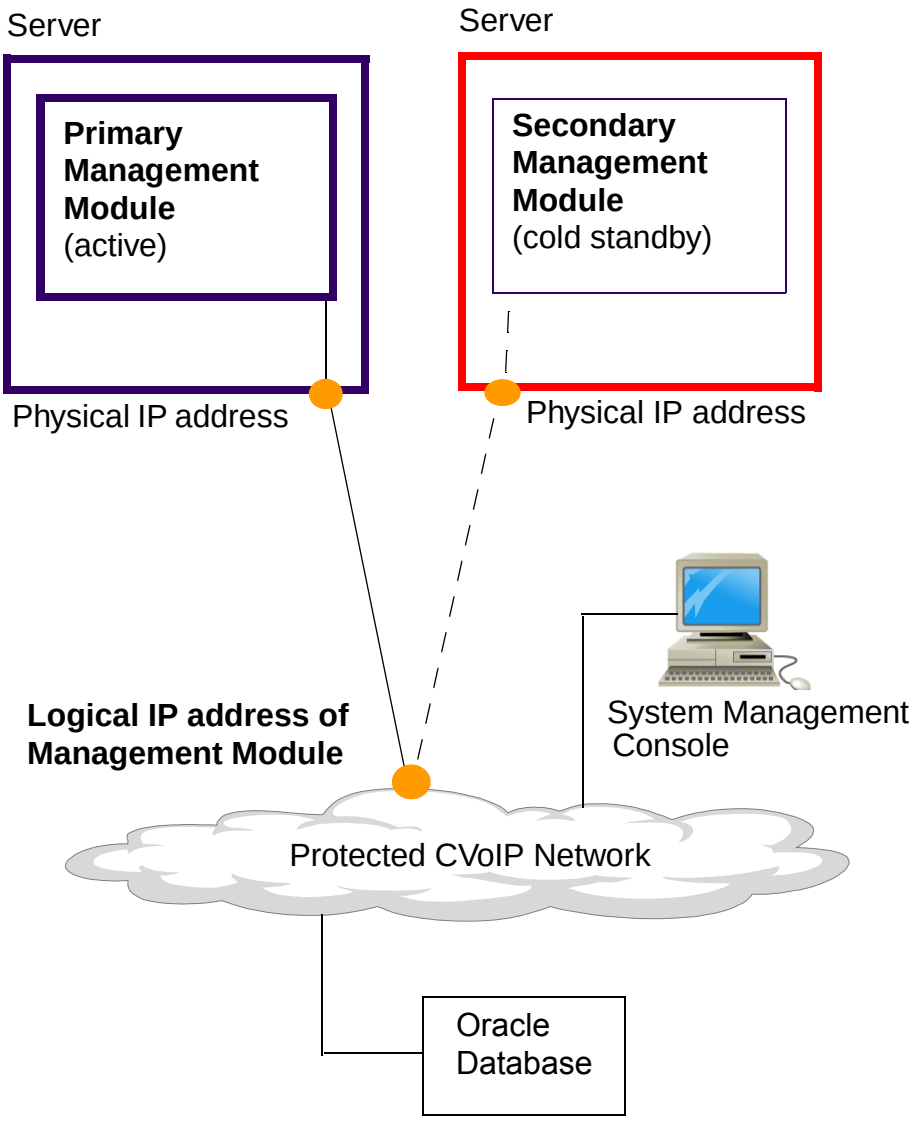
Figure 1 Connection lost dialog box

The lost connection may or may not be an indication that the Management Module (SysMgr) component or its hosting server has failed. Administrators need to perform basic connection troubleshooting to ensure the fault is not a network or other problem.

Manual failover in a redundant configuration

In a redundant configuration, two servers host the Management Module software. One server hosts the active primary Management Module and another the secondary in a cold standby state. If the primary Management Module or hosting server fails, a manual failover allows the transfer of the management operations to the secondary Management Module. The active Management Module component owns the logical IP address used to connect with the System Management Console. In addition, all the managed elements use the logical IP address to send logs, alarms, and OMs to the Management Module. A logical view of the arrangement is shown in the following figure.

Figure 2 Redundancy of Management Module - logical view



When the management server or primary Management Module fails, the System Management Console loses its connection. In addition, logs and alarms from the managed elements are not reported. To resolve this fault, an administrator needs to perform a manual failover to the secondary Management Module.

The manual failover process involves stopping the Management Module processes and releasing the logical IP address from the management server, and starting the processes on the server hosting the secondary Management Module. Both actions require the use of a Unix login account.

The Oracle database stores the system application and configuration data. The secondary Management Module retrieves the latest configuration data from the database when it becomes active. However, all information stored on the management server's local disk is not transferred during a manual failover. This information includes archived logs and holding OMs.

To facilitate this procedure, we recommend that administrators have a log book with the information (physical and logical IP addresses, login information) required to perform the failover.

Physical IP addresses of the Management Modules

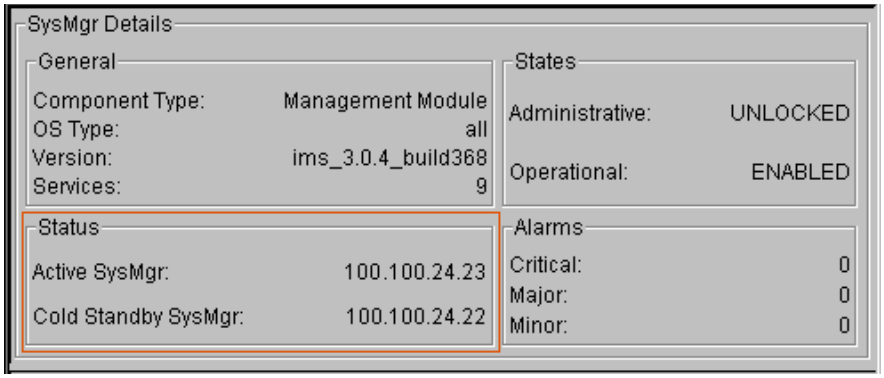
Administrators need to know the physical IP addresses of the servers hosting the primary (active) and secondary SysMgr components before performing a manual failover. The physical IP addresses of the active and cold standby Management Modules are displayed in the GIA of the System Management Console.

From the System Management Console

1 Select the **SysMgr** component in the system tree.

The status box of the GIA displays the physical IP addresses for the primary (active) and secondary (cold standby) Management Modules.

Figure 3 GIA showing the physical IP addresses of the Management Modules

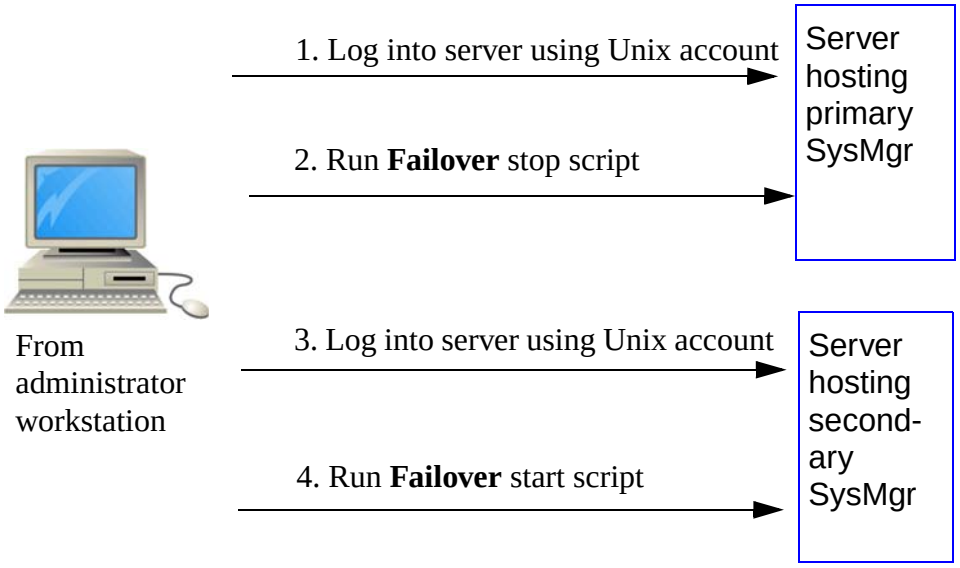


Performing a manual failover in a redundant configuration

When the SysMgr component fails, its associated processes and ownership of the logical IP address need to be stopped. Since the connection to the System Management Console is lost, administrators need to remotely log onto the servers from their workstation.

To log onto the servers, the administrators need to use the limited access account created for this procedure. The following figure shows the sequence of actions performed during the failover procedure.

Figure 4 Steps in performing a manual failover



See the following for the manual failover procedures:

- Stopping the Management Module processes
- Starting the cold standby Management Module
- Reverting back to the primary Management Module
- Failover impacts and recovery

Stopping the Management Module processes

Stop the primary Management Module if possible. If the hosting server is down, or in an isolated state, this will not be possible and administrators should proceed to the next step: Starting the cold standby Management Module.

from the administrator's workstation

1 Log onto the server running the active SysMgr component.

IP Address : <physical address of server>

Login ID : sysadmin

2 Navigate to the directory with the failover script.

```
cd /IMS/mgmtsvr/bin
```

3 Execute the failover shutdown script to stop SysMgr processes and release the logical IP address. The sudo command gives an administrator root privileges limited to running the failover script.

```
sudo Failover.pl stop sysmgr
```

When the shutdown is finished, the screen will display the name and path of the log file associated with this event.

Starting the cold standby Management Module

When the backup SysMgr component is started, the Management Module logical IP address becomes associated with the newly active SysMgr. Once the logical IP address is up, administrators can reestablish the System Management Console connection.

from the administrator's workstation

1 Log onto the server hosting the secondary SysMgr component.

IP Address : <physical address of server>

Login ID : sysadmin

2 Navigate to the directory with the failover script.

```
cd /IMS/mgmtsvr/bin
```

3 Execute the failover startup script to start SysMgr processes and take ownership of the logical IP address.

```
sudo Failover.pl start sysmgr
```

When the startup is finished, the screen will display the name and path of the log file associated with this event.

Reverting back to the primary Management Module

The procedure to revert back to the primary Management Module is the reverse of the failover to the secondary.

from the administrator's workstation

1 Close the System Management Console connection.

2 Log into the server running the active secondary SysMgr component.

IP Address : physical address of the server

Login ID : sysadmin

3 Navigate to the directory with the failover script.

```
cd /IMS/mgmtsvr/bin
```

4 Execute the failover script to stop SysMgr processes and release the logical IP address.

```
sudo Failover.pl stop sysmgr
```

5 Log onto the management server hosting the main SysMgr component.

IP Address : physical address of management server

Login ID : sysadmin

6 Navigate to the directory with the failover script.

```
cd /IMS/mgmtsvr/bin
```

7 Execute the failover script to start SysMgr processes and take ownership of the logical IP address.

```
sudo Failover.pl start sysmgr
```

8 Reestablish the System Management Console connection.

Failover impacts and recovery

Stopping the primary Management Module may not be possible due to network isolation of the management server.

Impact:

A remote login session may not be possible if the server is in a network isolated state. The secondary Management Module can still be started and take ownership of logical IP address. However, if the primary Management Module comes back online while the secondary is running, there will be conflicts between the now two active components.

Recovery:

Administrators need to promptly shutdown one of the two active components. If possible, the administrator should try to connect to the management server through the terminal server and power down the server. As a last resort, physically cycle down the power on the management server until the backup Management Module is stopped.

Restarting a failed Management Module in a non-redundant configuration

In a non-redundant configuration, the single instance of the Management Module shares a server with one or more active CVoIP components.

If the Management Module fails, watch-dog processes will attempt to restart the Management Module three times. If this doesn't work,

administrators can attempt to restart the Management Module using one of two approaches: log into the server and stop/start the SysMgr using command line interface (CLI) commands, or perform a server reset using the System Management Console.

The preferred method of restarting the Management Module is to execute stop/start commands while logged onto the sever. This method will not affect the other applications also running on the server.

from a workstation

1 Log into the server hosting the Management Module.

2 Navigate to the following directory.

```
cd /IMS/mgmtsvr/bin/mgmtsvr
```

3 Execute the following commands.

```
MgmtSvrShutdown.pl
```

```
MgmtSvrConfigSetup.pl
```

An alternate but less preferred method, is to reset the hosting server using the System Management Console. This method will affect all other applications also running on the server, and the System Management Console will lose its connection.

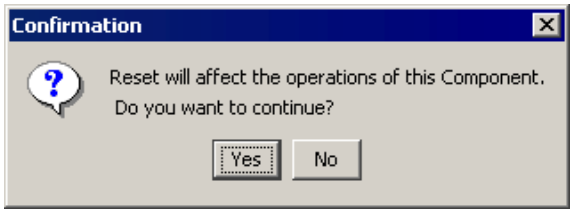
from the System Management Console

1 Select the server hosting the Management Module (SysMgr) in the system tree.

2 In the menu bar, select Operations > Reset.

The Confirm reset prompt opens.

Figure 5 Confirm reset prompt



3 Click Yes.

Logs overview

Logs are events that occur during the operation of the service components. They are used to record information related to an event so

that it may be analyzed at a later point in time. Every log event is captured and archived in Standard (STD) format to disk on the server hosting the Management Module.

There are two types of logs users can request to view from the System Management Console: Current and Archived. Current logs are a live stream of logs/events being reported to the Management Module. As the logs are received, they are saved to the current (*.active) log file. After a configured period of time, or when the file reaches a configured size in kilobytes, the log file is closed and renamed (rotated) to an archived log file and a new current log file is opened.

The directory path to the logs on the Management Server is

```
/IMS/tss/data/oss/Log/b643net/MgmtSite/<ServCompNam
e>/0/<filename>
```

Where:

<ServCompName> is the name of the service component that originated the logs.
<filename> is the log file name.

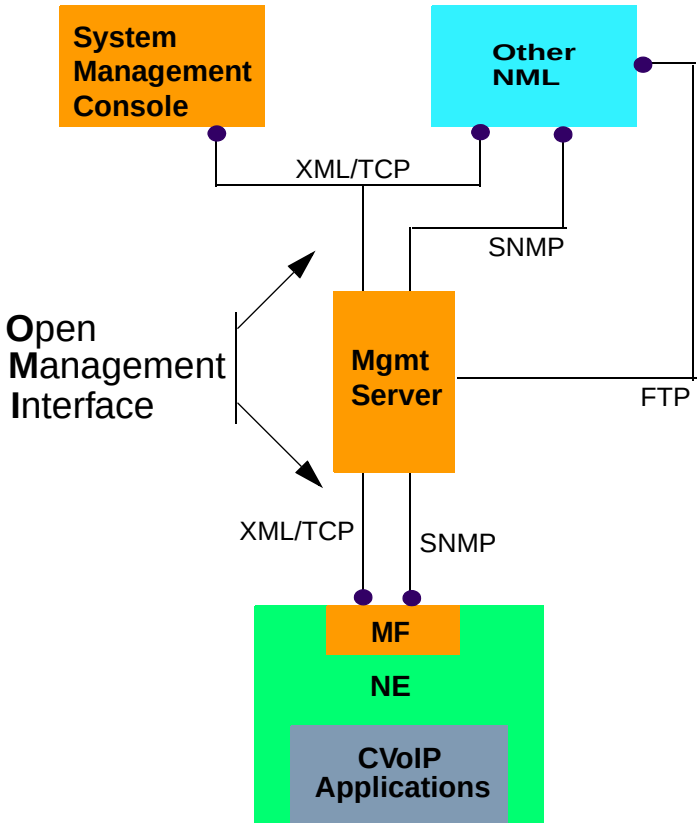
Alarms overview

Once in operation, system elements have the ability to raise and clear alarms/faults. As faults occur, alarms are generated by the element and sent to the Management Module component. Once at the Management Module, administrators can view the alarms using the System Management Console's alarm browser.

When an alarm is raised, it is added to a list of active alarms. The alarm remains on the active list until it is resolved. Once the problem is resolved, the alarm is cleared and removed from the list of active alarms.

The following diagram shows a logical view of the alarm framework interfaces for the CVoIP components.

Figure 6 CVoIP component alarm framework interfaces



See the following topics for more alarm information:

- Information on Alarms
- Alarm severity classification
- Alarms recorded as log entries
- Alarms integration with NML using SNMP

Information on Alarms

The information displayed in the alarm browser is dependent on the element selected in the hierarchy tree. For example, if a server is selected, the alarm browser shows the alarms for all the components hosted on the server, if a component is selected only the alarms generated by the component services are displayed. Administrators can launch more than one browser, allowing them to view alarms for specific elements separately.

All alarms viewed in the alarm browser give the following information:

Table 1 Alarm information displayed in the alarm browser

Alarm attribute	Description
Timestamp	time when the alarm was raised
Severity	severity assigned to the alarm (see Alarm severity classification)
Originator	service originating the alarm
Alarm Name	name of the alarm
ProbableCause	the general problem causing the alarm
Family Name	managed object family originating the alarm
AlarmNumber	the number identifier of the alarm
CLR	Indicates whether the alarm has been cleared. When cleared, a trash icon appears in the column.

Additional information is included to help identify the service originating the alarm when the following nodes are selected in the hierarchy tree:

- System: alarm browser also displays the site, server, and component hosting the alarm originator
- Site: alarm browser also displays the server and component hosting the alarm originator
- Server: alarm browser also displays the component hosting the alarm originator

Alarm severity classification

Associated with alarms is a severity level that indicates how serious the problem is to the system. Alarm severity is also displayed as a color in the hierarchy tree and alarm browser. When a portion of the hierarchy tree is collapsed, the color shown represents the most severe alarm of an element in the collapsed tree.

Alarm severity is classified according to descriptions in the following table.

Table 2 Alarm severity classification

Severity	Color	Description
Critical (5)	Red	Application is unable to provide desired functionality
Major (4)	Orange	Application is having difficulty providing desired functionality
Minor (3)	Yellow	Application has a problem not yet affecting functionality
Warning (2)	Green	A nonservice-affecting problem has occurred

Alarms recorded as log entries

Every alarm generates an associated log. Administrators view alarm information in log format using the log browser. The format of an alarm, viewed from the log browser, is different from the format that is displayed through the alarm browser.

Alarm logs use the following format:

```
<SrvComp> <Severity> <AlarmIdentifier> <TimeStamp>
<MiscInfo> <AlarmDescription>
```

Where:
`<SrvComp>` service component generating alarm
`<Severity>` severity number of the alarm, represented by asterisks. The asterisks represent the severity offset by two. For example, a critical alarm (severity of 5) displays *** (3 asterisks) in the log, a minor alarm (severity of 3) displays * (1 asterisk) in the log.
`<AlarmIdentifier>` alarm family name and number
`<TimeStamp>` date and time alarm occurred
`<MiscInfo>` miscellaneous information associated with alarm
`<AlarmDescription>` alarm description

The following is an example of a log produced for a critical alarm:

```
app001 *** IMSA799 JUL10 13:21:35 0707 TBL INST0
OssMgmtAgent.administrationAndOperationalState:
[severity=CRITICAL][probableCause=software error]
[addedText=Object DISABLED]
```

Alarms integration with NML using SNMP

Network administrators can integrate alarms generated by CVoIP managed objects into their current Network Management Layer (NML) manager.

Alarm generating events report to the SNMP (Simple Network Management Protocol) manager registered with the system. A Management Information Base (MIB) definition is available for integration of CVoIP service component alarms.

Administrators access the SNMP management options from the System Management Console.

Alarm descriptions

The following table lists all the families of alarms reported to the Management Module and viewed in the System Management Console. Click on the link to view the component's alarm descriptions.

Table 3 Alarm families and their originating modules

Short name	Long name*	Component(s) or services generating alarm
DBF	DFB-OAM	DatabaseFactory Refer to CVoIP Database Module Basics for alarm descriptions.
IMD	IMDB	In Memory Database (IMDBManager) Refer to CVoIP Database Module Basics for alarm descriptions.
IMS	IMS-OAM	OAM framework IMS (OAM framework) alarm descriptions
LCK	LCKEY	License Key Manager LCK (License Key Manager) alarm descriptions
MS	MS-OAM	Platform SNMP Manager MS (Platform SNMP Manager) alarm descriptions
ODB	ORCL-DB	Oracle DatabaseBase Refer to CVoIP Database Module Basics for alarm descriptions.

* The long name is used in the FamilyName column of the alarm browser.

Table 3 Alarm families and their originating modules

Short name	Long name*	Component(s) or services generating alarm
ORCL	ORCL	Oracle Refer to CVoIP Database Module Basics for alarm descriptions.
OSS	OSS-OAM	OSS agent OSS (OSS Agent) alarm descriptions
RECS	RECS	Recording System RECS (Recording System) alarm descriptions
RTP	RTP-OAM	BladeSimUDPIOControllerFactory Refer to CVoIP RTP Media Portal Basics for alarm descriptions.
SLOG	SLOG-OAM	SysLogMonitor OAM SLOG (SysLogMonitor OAM) alarm descriptions
SNMP	SNMPTRAP	SNMP

* The long name is used in the FamilyName column of the alarm browser.

SLOG (SysLogMonitor OAM) alarm descriptions

SysLogMonitor alarms are raised by Solaris server alert messages. Administrators configure the number of messages for each alarm and the alarm's life time in the alarm browser in the Management Module component's SysLogMonitor service. See the section Server alert

message configuration for information on how to configure server alert messages.

Table 4 SLOG921

Alarm Name:	SysLog Alarm
Alarm ID:	SLOG921
Category:	EQUIPMENT
Severity:	Critical, Major, Minor, Warning
Description:	This alarm reports an incident recorded in the /var/adm/messages file by the Solaris operating system. The incidents that are reported by this alarm are the ones labeled with 1) *.emerg and *.alert (to be a critical alarm) 2) *. crit (to be a major alarm) 3) *. Err (to be a minor alarm) 4) *.notice and *.warning (to be a warning alarm)
Corrective Action:	See more info in /var/adm/messages and take appropriate administrative measures if needed. The alarm is auto-cleared at the end of the configured SysLog alarm life time.

IMS (OAM framework) alarm descriptions

IMS alarms can be raised by all components with the exception of the following: IMS940, IMS943, IMS944, and IMS945. These four alarms are only raised by the iPlanet Monitor and Oracle Monitor components.

Table 5 IMS711

Alarm Family:	IMS
Alarm ID:	IMS711
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Initialization fault - Error reading configuration.
Corrective Action:	If alarm persists, contact your next level of support.

Table 6 IMS712

Alarm Family:	IMS
Alarm ID:	IMS712
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Initialization fault - Error allocating internal resources.
Corrective Action:	In the case of waiting for dependencies, user should allow for those dependencies to finish their own startup sequence, in which case, if successful, this alarm would be cleared automatically. If alarm persists, contact next level of support.

Table 7 IMS713

Alarm Family:	IMS
Alarm ID:	IMS713
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Initialization fault - Error allocating external resources, which are not created by this component.
Corrective Action:	In the case of waiting for dependencies, user should allow for those dependencies to finish their own startup sequence, in which case, if successful, this alarm would be cleared automatically. If alarm persists, contact next level of support.

Table 8 IMS714

Alarm Family:	IMS
Alarm ID:	IMS714
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Initialization fault - Error initiating communications with other objects.
Corrective Action:	If alarm persists, contact your next level of support.

Table 9 IMS721

Alarm Family:	IMS
Alarm ID:	IMS721
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Initialization fault - Error reading configuration. This alarm is equivalent to IMS711 but is raised for a managed object (MO) that is generated by a different base program.
Corrective Action:	In the case of waiting for dependencies, user should allow for those dependencies to finish their own startup sequence, in which case, if successful, this alarm would be cleared automatically. If alarm persists, contact next level of support.

Table 10 IMS722

Alarm Family:	IMS
Alarm ID:	IMS722
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Initialization fault - Error allocating internal resources. This alarm is equivalent to IMS712 but is raised for an managed object that is generated by a different base program.
Corrective Action:	In the case of waiting for dependencies, user should allow for those dependencies to finish their own startup sequence, in which case, if successful, this alarm would be cleared automatically. If alarm persists, contact next level of support.

Table 11 IMS723

Alarm Family:	IMS
Alarm ID:	IMS723
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Initialization fault - Error allocating external resources. This alarm is equivalent to IMS713 but is raised for an managed object that is generated by a different base program.
Corrective Action:	In the case of waiting for dependencies, user should allow for those dependencies to finish their own startup sequence, in which case, if successful, this alarm would be cleared automatically. If alarm persists, contact next level of support.

Table 12 IMS724

Alarm Family:	IMS
Alarm ID:	IMS724
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Initialization fault - Error initiating communications. This alarm is equivalent to IMS714 but is raised for an managed object that is generated by a different base program.
Corrective Action:	In the case of waiting for dependencies, user should allow for those dependencies to finish their own startup sequence, in which case, if successful, this alarm would be cleared automatically. If alarm persists, contact next level of support.

Table 13 IMS725

Alarm Family:	IMS
Alarm ID:	IMS725
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Initialization fault - Waiting for critical dependencies.
Corrective Action:	In the case of waiting for dependencies, user should allow for those dependencies to finish their own startup sequence, in which case, if successful, this alarm would be cleared automatically. If alarm persists, contact next level of support.

Table 14 IMS726

Alarm Family:	IMS
Alarm ID:	IMS726
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Initialization incomplete.
Corrective Action:	If alarm persists, contact your next level of support.

Table 15 IMS751

Alarm Family:	IMS
Alarm ID:	IMS751
Category:	PROCESSING_ERROR
Severity:	Minor
Description:	Application currently runs using old configuration data. Application needs to be restarted in order to use its newly modified data.
Corrective Action:	Current application needs to be restarted.

Table 16 IMS752

Alarm Family:	IMS
Alarm ID:	IMS752
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Validation failed during configuration.
Corrective Action:	Record the configuration related error and contact your next level of support.

Table 17 IMS753

Alarm Family:	IMS
Alarm ID:	IMS753
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Reading configuration failed.
Corrective Action:	Record the configuration related error and contact your next level of support.

Table 18 IMS754

Alarm Name:	IMS
Alarm ID:	IMS754
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	Reading configuration failed at startup.
Corrective Action:	Record the configuration related error and contact your next level of support.

Table 19 IMS782

Alarm Name:	IMS
Alarm ID:	IMS782
Category:	PROCESSING_ERROR
Severity:	Minor
Description:	Waiting for all managed objects to become LOCKED or DISABLED.
Corrective Action:	No action required.

Table 20 IMS783

Alarm Name:	IMS
Alarm ID:	IMS783
Category:	PROCESSING_ERROR
Severity:	Major
Description:	One or more dependencies are unavailable on current managed object.
Corrective Action:	If alarm persists, contact your next level of support.

Table 21 IMS784

Alarm Name:	IMS
Alarm ID:	IMS784
Category:	PROCESSING_ERROR
Severity:	Critical
Description:	One or more critical dependencies are unavailable on current managed object.
Corrective Action:	Ensure the connections to other components are up and the configuration is correct. If alarm persists, contact your next level of support

Table 22 IMS940

Alarm Name:	IMS
Alarm ID:	IMS940
Category:	QUALITY_OF_SERVICE/ENVIRONMENT
Severity:	Major
Description:	Validation of gauge configuration data failed.
Corrective Action:	Using System Console GUI, modify the configuration item values for the corresponding invalid thresholds and then dynamically update the application. When correction is made, the alarm is cleared automatically.

Table 23 IMS943

Alarm Name:	IMS
Alarm ID:	IMS943
Category:	QUALITY_OF_SERVICE/ENVIRONMENT
Severity:	Warning
Description:	<Component_Name>.<theMeasure> exceeds or equals the First Positive Going Threshold.
Corrective Action:	Obtain more resources or reduce the usage. The alarm clears automatically when usage moves below the threshold.

Table 24 IMS944

Alarm Name:	IMS
Alarm ID:	IMS944
Category:	QUALITY_OF_SERVICE/ENVIRONMENT
Severity:	Minor
Description:	<Component_Name>.<theMeasure> exceeds or equals the Second Positive Going Threshold
Corrective Action:	Obtain more resources or reduce the usage.

Table 25 IMS945

Alarm Name:	IMS
Alarm ID:	IMS945
Category:	QUALITY_OF_SERVICE/ENVIRONMENT
Severity:	Major
Description:	<Component_Name>.<theMeasure> exceeds or equals the Maximum Positive Going Threshold
Corrective Action:	Obtain more resources or reduce the usage.

MS (Platform SNMP Manager) alarm descriptions

MS alarms are raised by the managed servers.

Table 26 MS101

Alarm Name:	Host not reachable
Alarm ID:	MS101
Category:	COMMUNICATIONS
Severity:	Critical
Description:	The Host node cannot be reached. The node may be down or invalid IP address.
Corrective Action:	Ensure that SNMP agent is running on the host, if not, start the agent. If problem persists, contact your next level of support.

Table 27 MS102

Alarm Name:	Agent not reachable
Alarm ID:	MS102
Category:	COMMUNICATIONS
Severity:	Critical
Description:	The SNMP agent on the server cannot be reached.
Corrective Action:	Ensure that SNMP agent is running on the host, if not, start the agent. If this problem persists, contact your next level of support.

Table 28 MS103

Alarm Name:	SNMP agent on the server cannot be reached
Alarm ID:	MS103
Category:	COMMUNICATIONS
Severity:	Critical
Description:	The SNMP agent on the server cannot be reached.
Corrective Action:	Ensure the host IP and the port number are specified correctly. Check that the terminal server is up and/or the port is not already in use. If this problem persists contact your next level of support.

Table 29 MS901

Alarm Name:	CPU Util Exceeds Threshold
Alarm ID:	MS901
Category:	QUALITY_OF_SERVICE/EQUIPMENT/ENVIRONMENT
Severity:	Minor/Major/Critical
Description:	This Alarm is raised whenever any of the CPUs on the platform exceed the utilization threshold specified.
Corrective Action:	If the problem persists, contact your next level of support.

Table 30 MS902

Alarm Name:	Interface Utilization Threshold exceeded
Alarm ID:	MS902
Category:	QUALITY_OF_SERVICE/EQUIPMENT/ENVIRONMENT
Severity:	Minor/Major/Critical
Description:	This Alarm is raised whenever I/O interface on the platform exceed the utilization threshold specified.
Corrective Action:	If problem persists, contact your next level of support.

Table 31 MS903

Alarm Name:	Disk Utilization Threshold exceeded
Alarm ID:	MS903
Category:	QUALITY_OF_SERVICE/EQUIPMENT/ENVIRONMENT
Severity:	Major/Critical
Description:	This Alarm is raised whenever disk usage on the platform exceeds the utilization threshold specified.
Corrective Action:	Check for available disk space in the given partition and free up disk space. Check for disk errors. If problem persists, contact your next level of support.

Table 32 MS904

Alarm Name:	Memory Utilization Threshold exceeded
Alarm ID:	MS904
Category:	QUALITY_OF_SERVICE/EQUIPMENT/ENVIRONMENT
Severity:	Minor/Major/Critical
Description:	This Alarm is raised whenever memory on the platform exceeds the utilization threshold specified.
Corrective Action:	Increase physical memory and/or virtual memory size. If problem persists, contact your next level of support.

Table 33 MS905

Alarm Name:	Interface out of service
Alarm ID:	MS905
Category:	QUALITY_OF_SERVICE/EQUIPMENT/ENVIRONMENT
Severity:	Major/Critical
Description:	This Alarm is raised whenever an interface card is out of service.
Corrective Action:	Ensure the availability of the specific interface card of the server.

OSS (OSS Agent) alarm descriptions

OSS alarms are raised by the the OSS agent of the Management Module (SysMgr component).

Table 34 OSS101

Alarm Name:	OMI Connection Failure
Alarm ID:	OSS101
Category:	COMMUNICATIONS
Severity:	Major
Description:	Lost communication with host: {host} at port {port}. Raised when an OSS Agent fails to connect to remote OMI Agent.
Corrective Action:	Start the remote application. If problem persists, contact your next level of support.

RECS (Recording System) alarm descriptions

RECS alarms are raised by the recording system of each component. The recording system is not a service.

Table 35 RECS211

Alarm Family:	Recording System Alarm
Alarm ID:	RECS211
Category:	RESOURCE
Severity:	Critical
Description:	The recording system is unable to open the file path.
Corrective Action:	Check the directory structure and its permissions.

Table 36 RECS213

Alarm Name:	Recording System Alarm
Alarm ID:	RECS213
Category:	RESOURCE
Severity:	Critical
Description:	The recording system is unable to write a record to the current active file.
Corrective Action:	Check the directory, file permissions, and disk space usage.

SNMP (SNMP) alarm descriptions

SNMP alarms are raised by the components Management Module and Oracle Monitor components.

Table 37 SNMP101

Alarm Name:	SNMP Agent Unreachable
Alarm ID:	SNMP101
Category:	COMMUNICATIONS
Severity:	Critical
Description:	SNMP Agent not reachable, check that if the agent is up at: ipAddress = <IpAddress>, Port = 9162 or the read-only community string is consistent with the expected value.
Corrective Action:	Ensure that SNMP agent is running on the host, if not, start the agent. Otherwise, ensure that the read-only community string is consistent with the expected value. If this problem persists, contact your next level of support.

Table 38 SNMP701

Alarm Name:	SNMP Trap
Alarm ID:	SNMP701
Category:	PROCESSING_ERROR
Severity:	Minor
Description:	Unknown V1 or V2 SNMP Trap Received.
Corrective Action:	Ensure both the SNMP listener and the SNMP agent are running. After the situation is corrected, must restart the component to clear the alarm. The alarm and its clearing may take a while to occur due to the snmp polling and networks delays.

LCK (License Key Manager) alarm descriptions

The following alarms are raised by the License Key Manager.

The threshold alarms are used for total subscribers, advanced screening subscribers, presence subscribers, and network call log subscribers. Threshold alarms may require an update to the license key to allow more subscribers. Threshold alarms clear when the total number of licensed entities falls below the threshold limit. The procedure to update a license key is documented in the CVoIP System Management Console User Guide.

Table 39 LCK404

Alarm Name:	LKEY_Threshold_Critical
Alarm ID:	LCK404
Category:	THRESHOLD
Severity:	Critical
Description:	A license Key keycode is at its limit.
Corrective Action:	Update License Key to support more resources.

Table 40 LCK405

Alarm Name:	LKEY_Threshold_Major
Alarm ID:	LCK405
Category:	THRESHOLD
Severity:	Major
Description:	A license Key keycode is at 90% of its licensed limit.
Corrective Action:	Update License Key to support more resources.

The following table identifies log messages resulting from license key problems. These can be used if reporting License key problems to the next level of support.

Table 41 License key error logs

Log message	Cause	Action required
Error occurred decrypting License Key file	Indicates the License Key file could not be decrypted. This can be caused by: an invalid License Key file, incompatible version of the License Key file, or a corrupt License Key file.	Ensure that the License Key is intended for the target system. Ensure that the License Key file is not corrupted. Otherwise contact your next level of support and provide them with the header information located in the first line of the License Key file.
License Key file not found	Indicates the system could not find the License Key file.	Refer to the installation and commissioning documentation for instruction on entering a License Key file.
Could not retrieve License Key from Database	Indicates the system could not retrieve the License Key from the database.	Ensure that database connectivity can be established with the database.

Table 41 License key error logs

Log message	Cause	Action required
Could not update License Key, reverting to original	Indicates the License Key on the target system could not be updated. This can occur if the License Key is intended for a major release update, the MAC addresses on the target system do not match the MAC addresses on the License Key file, or if a software error occurred during the License Key update process. The system reverts back to the original license key.	Ensure that the License Key is intended for the target system. Ensure that the License Key file is not corrupted. Otherwise contact your next level of support and provide them with the header information located in the first line of the License Key file.
Could not update Database License Key file	Indicates the License Key file has been validated by the system, but the system could not update the License Key on the database.	Ensure that the target system has connectivity to the database.
Error occurred parsing License Key file	An error occurred during validation of the License Key file.	Ensure that the License Key file is not corrupted. Otherwise contact your next level of support and provide them with the header information located in the first line of the License Key file.
Error occurred validating License Key MAC Addresses	Indicates an error occurred validating the License Key file MAC addresses against the target system.	Ensure that the License Key is indented for the target system. Ensure that the License Key file is not corrupted. Otherwise contact your next level of support and provide them with the header information located in the first line of the License Key file.
Error occurred getting node MAC Addresses	An error occurred retrieving the target nodes MAC addresses via the operating system.	Ensure that the License Key is intended for the target system.
The License Key MAC addresses do not match this nodes MAC addresses	Indicates the License Key MAC addresses do not match the target nodes MAC addresses.	Ensure that the License Key is intended for the target system.

Table 41 License key error logs

Log message	Cause	Action required
License Key upgrade failed. New License Key required for major release upgrade	Indicates the License Key upgrade failed because the supplied License Key was intended for a system with a newer software release. The supplied License Key is not compatible with the target system installed software.	Upgrade target system software release or contact your next level of support.
Error occurred parsing node MAC Addresses	An error occurred. Query the operating system for it's MAC addresses.	Ensure that the License Key is intended for the target operating system.

Configuration management

Topics in this chapter

Configuration strategy and tools

Deployment personnel perform the manual installation and configuration of the Management Module. The installation process adds the management site, management server, and Management Module component (labelled *SysMgr* in the system tree). Only after the Management Module is installed and operational, can administrators interact with the system elements using the System Management Console.

All the service properties of the Management Module are pre-configured with default values. Only the SysLogMonitor service can be modified after deployment. The Database service has properties administrators can query but not modify.

Sever alert patterns monitored by the Syslog monitor are configured on the server hosting the Management Module. Information on configuring server alert patterns is documented in the section Server alert message configuration.

Optional configuration tasks

Log and operational measurement (OM) file rotation parameters are typically configured at the system level. However, they can also be configured with values for either a specific server or component. Information on configuring the rotation parameters are documented in the *CVoIP System Management Console User Guide*.

SNMP community string values for a server can be changed from the default ‘public’ to some other value for network security reasons. Once configured for a server, it applies this community string value to SNMP message traffic of the hosted components. Information on configuring the community string is documented in the *CVoIP System Management Console User Guide*.

Modifying the SysLogMonitor service properties

The SysLogMonitor service raises an alarm when system alert message logs are generated by servers running Solaris operating systems. The alarm clears after the configured interval.

The Management Module component cannot be locked. To enable the modify option, the following procedure permits the locking of the single service. Locking the SyslogMonitor has no impact on other services.

from the System Management Console

1 Select the **SysLogMonitor** service in the system tree.

2 From the menu bar, select **Operations** > **Lock.**

The Confirm prompt opens.

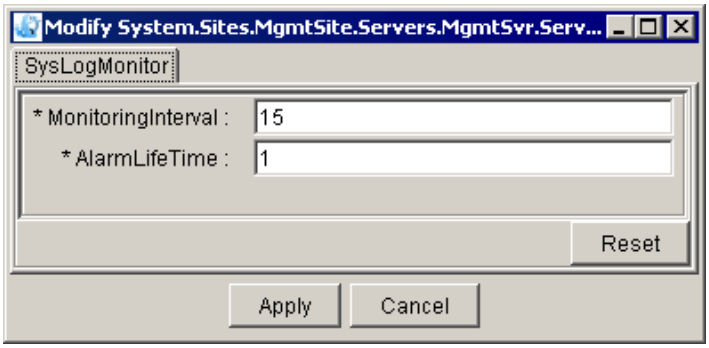
3 Confirm the lock, click **Yes.**

The administrative state of the SysLogMonitor changes to locked. In a locked administrative state, no new server alarms are generated and sent to the System Management Console.

4 From the menu bar, select **Configuration** > **Modify.**

The SysLogMonitor configuration widow opens.

SysLogMonitor configuration window



5 Modify the configuration, entering new values into the property fields.

SysLogMonitor tab property descriptions

Property	Format [default]	Description [range]
MonitoringInterval	Integer [15]	Defines how often (in minutes) the log monitor will raise an alarm if there is new ‘alert msgs’ in the /var/adm/messages file [15-1440 minutes].
AlarmLifeTime	Integer [1]	Defines the time period (in minutes) before the alarm is auto cleared [1-14].

6 Click **Apply**.

7 From the menu bar, select **Operations** > **Unlock**.

The administration state changes to unlocked.

Server alert message configuration

Alert messages are generated by Solaris operating systems running on the system's Sun servers. The alert messages are normally logged to the local `/var/adm/messages` directory on the server. However, the server's logs can be routed to the server hosting the Management Module. Once on this server, the Management Module's SysLogMonitor will generate alarms when messages from monitored servers match a configured alert pattern. Administrators can then view the alarms in the System Management Console alarm browser.

The alert patterns and routing are configured during system installation and commissioning. However they can be modified to reflect specific system administration requirements after installation. In addition, a server can be added to be monitored. See the following procedures for more information:

- Changing the alert messages to monitor
- Adding a server to monitor

Information on modifying the SysLogMonitor's parameters is described in the section Modifying the SysLogMonitor service properties.

Changing the alert messages to monitor

Modification of alert patterns requires root access to the server hosting the Management Module, which may require the involvement of your next level of support. For these procedures, the server hosting the Management Module will be called the management server for clarification.

Alert patterns definitions are located on the management server in the file:

```
/IMS/mgmtsvr/data/mgmtsvr/config/SysLogPatterns.dat
```

Each alert pattern is defined in the following format:

```
<severity>;<facility>.<level>;<facility>.<level>;...
```

Where:

<severity>	A numeric value of the alert severity level used to map it to an alarm severity. The mapping is as follows: 4 = Critical alarm 3= Major alarm 2 = Minor alarm 1 = Warning
<facility>	Indicates a Solaris monitored facility such as daemon, kernel, etc. Use an asterisk (*) to include all facilities. See the Solaris documentation for the complete list of facilities and their descriptions.
<level>	The level of alert message as defined by Solaris such as emerg, crit, etc. See the Solaris documentation for the complete list of alert levels.

Example
4;daemon.emerg;kernal.emerg;*.alert

In the above example, a critical alarm is raised for the server's daemon and kernel facilities with messages with emerg severity level, and all facility messages with alert severity level.

The default patterns and alarm mappings are listed in the following table.

Default alert patterns monitored

Alert pattern <severity>	Default patterns being monitored	Management Console alarm severity
4	*.emerg; *.alert	Critical
3	*.crit	Major
2	*.err	Minor
1	*.warning; *.notice	Warning

Note: The <severity> assigned to an alert pattern is not the same as the numeric severity level of the alarm.

from an administrator workstation

1. Log onto the management server. This requires root access.
2. Open the SysLogPatterns.dat file located on the management server located in the following directory path:

   /IMS/mgmtsvr/data/mgmtsvr/config/SysLogPatterns.dat
3. Modify the alert pattern definitions.
4. Log off the management server.

To begin monitoring the new alert patterns, the SysLogMonitor service needs to be restarted using a lock - unlock sequence.

from the System Management Console

1. Select the **SysLogMonitor** service in the system tree.
2. From the menu bar, select **Operations** > **Lock.**

   The SysLogMonitor service goes into an locked administrative state.
3. From the menu bar, select **Operations** > **Unlock.**

   The SysLogMonitor restarts and begins raising alarms based on the updated alert pattern definitions.

Adding a server to monitor

Monitored servers are configured during system installation and commissioning. Adding a server to monitor requires manual configuration of the server's syslog file to route alerts to the management server or Management Module component. This configuration requires root access to the added server which may require the involvement of your next level of support.

from an administrator workstation

1. Log onto the server that is being added. This requires root access.
2. Modify the /etc/syslog.conf file on the server, adding the line:

   ***.emerg;*.alert;*.crit;*.err;*.warning;*.notice @<mgmt_IP>**

   where:

<mgmt_IP> is the IP address the alerts are routed to. The following table lists the IP address based on the specific network configuration.

IP address to route syslog messages

Management Server network scenario	Use the following IP address to route the alerts
Single management server without IP multipath enabled	Machine IP address of the management server
IP multipath enabled but no management module failover (i.e. single management server)	Logical IP address of the management server
IP multipath enabled and secondary management module (i.e. more than one server hosting the Management Module component software)	Logical IP address of the SysMgr component. This IP address is also used in the `/var/adm/messages` directory of the management servers.
Note: Use the private IP address in network that uses both private and public IP addresses.	

This default configuration routes the logs for all facilities generating alerts with the severity of emerg, alert, crit, err, warning, and notice to the management server.

3 Stop and restart the Syslog daemon to apply the changes.

```
prompt> /etc/init.d/syslog stop
prompt> /etc/init.d/syslog start
```

4 Log off the server.

Querying the Database service configuration

The Database service provides the interface that allows communication between the Management and Database modules. The connections between the Management Module and the Database carry configuration information using the SQL over JDBC protocol. The information includes data such as query requests and configuration updates. For information on modifying the Database configuration, refer to *CVoIP Database Module Basics*.

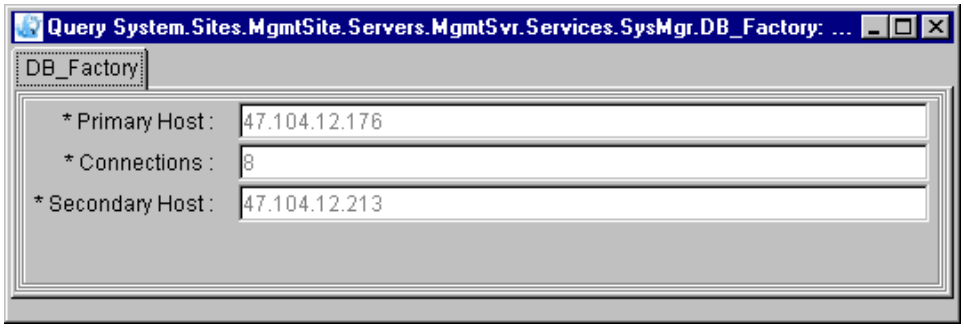
from the System Management Console

1 Select the **Database** service of SysMgr in the system tree.

2 From the menu bar, select **Configuration** > **Query**.

The DB_Factory query configuration window opens.

Database factory query window



Database service properties

Property	Format	Description
Primary Connection	IP address	IP address of primary database.
Connections	Type: Integer Range: 5 - 256	The number of database connections.
Secondary Host	IP address	IP address of replicated database.

3 To close the window, click the window's close button.

Accounting

Management Module configuration and operations have no impact or involvement in accounting functions.

Performance management

Topics in this chapter

Performance monitoring strategy and tools

Administrators use the System Management Console to monitor performance metrics of the Management Module and its hosting server. The general information area (GIA) of the System Management Console provides a view of the operational state of the Management Module and its services. The GIA also displays metrics of the server hosting the Management Module. Operational measurements for the Management Module processes, consisting of counters and gauges, are viewed in the OM browsers of the System Management Console.

For information on using the System Management Console, refer to the *CVoIP System Management Console User Guide*.

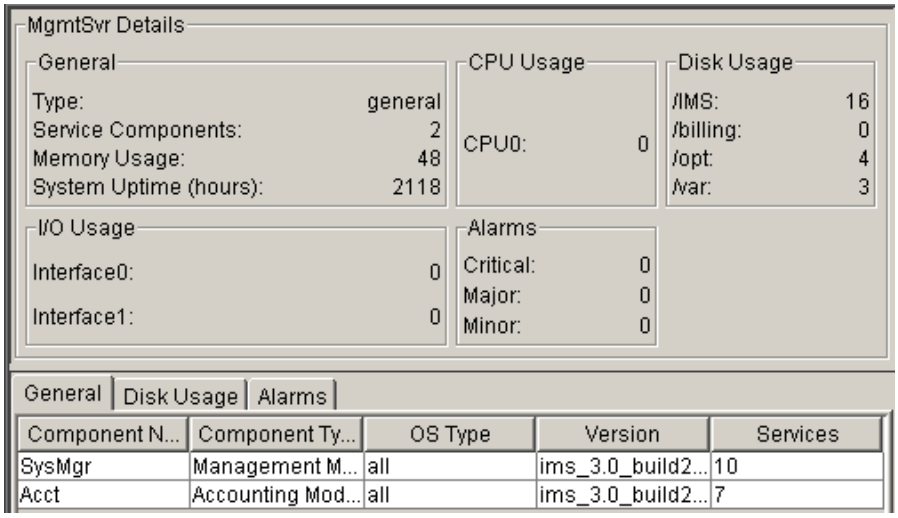
General information area

When administrators select the Management Module component in the system hierarchy tree, the GIA displays a snapshot of the operational and administrative states of the component and its services.

When administrators select the server hosting the Management Module in the hierarchy tree, the GIA displays server performance information including:

- CPU usage
- Disk usage
- Input/output usage
- Memory usage

Figure 1 GIA display when the Management Module's hosting server is selected



Operational measurements

Operational measurements consist of counters and gauges monitoring the activity of the Management Module processes. The OM groups associated with the Management Module are the following:

- OSS Mgmt Agent OM
- Managed element OM
- SysMgr (Management Module) OM

Operational measurement files generated by the Management Module are viewed using System Management Console OM browsers. The current Management Module OM file is viewed in the Active OM Browser. After the configured interval or file size, the active OM file is rotated out, going from an active to holding status.The holding files are viewable in the Holding Log Browser until the file retention period expires.

Typically, the configuration of OM file rotation periods is configured at the system level. However, they can also be configured at the server or component level. The procedure for configuring the OM rotation period is documented in the *CVoIP System Management Console User Guide*.

The OM file retention period is configured at a system level. The procedure for configuring the retention period is documented in the *CVoIP System Management Console User Guide*.

OSS Mgmt Agent OM

OMs of the OSS MgmtAgent group are generated by applications managed by the Management Module

Table 1 OSS Mgmt Agent

OM Name	Format	Definition
nrOfEventsReceived	Integer	Counter, indicating the number of state change events received by OssMgmtAgent from the internal framework. A state change by any managed element results in an event being sent to the OSS Mgmt Agent ME. The OSS Mgmt Agent processes these events by filtering out any duplicate events.
nrOfMessagesSentToTCF	Integer	Counter, indicating the number of events sent by the OSS Mgmt Agent ME to the OSS TCF ME. The OSS Mgmt Agent only sends non-duplicated events to the TCF ME. The TCF ME broadcasts these state change events to all connected System Manager monitoring clients. It is noted that since the OSS Mgmt Agent filters events received from internal framework, the 'nrOfMessagesSentToTCF' should be less than or equal to 'nrOfEventsReceived'.
notifyQueueSize	Integer	The internal framework sends state change events to the OSS Mgmt Agent. The OSS Mgmt Agent queues these events before processing them (i.e. filtering them). At a periodic interval (the default being 1 second), the OSS Mgmt Agent processes events on its queue. The OM counts the number of events on the queue that are waiting to be processed by the OSS Mgmt Agent.

Managed element OM

The following OM groups are common to all applications:

- Mecomchn
- Mecommgr

Table 2 Mecomchn

OM Name	Format	OM description
inacthndir	Integer	Counter, number of Mailboxes that are in-active
bkmboxfull	Integer	Counter, number of Mailboxes that are full
eventssent	Integer	Counter, number of events sent through the ME communication channel
eventsrecd	Integer	Counter, number of events received through the ME communication channel
The mailbox in the OM description is a term used for the mechanism in which messages are "posted/delivered to" and "read/extracted from" for a given process (application).		

Table 3 Mecommgr

OM Name	Format	OM description
connreject	Integer	Counter, number of connections rejected by the ME communication manager
sendreject	Integer	Counter, number of Send msgs rejected by the ME communication manager

SysMgr (Management Module) OM

The SysMgr component (Management Module) generates operational measurements for the following groups:

- OssAgent
- System_Sites_MgmtSite_Servers_MgmtSvr_Services_Sysmgr_TrapDispatcher
- <SiteName> <ServerName>

Table 4 OssAgent

OM Name	Format	Definition
oss agent	Integer	Counter, number of System Management Console logins there have been to the management server

Table 5 System_Sites_MgmtSite_Servers_MgmtSvr_Services_Sysmgr_TrapDispatcher

OM Name	Format	Definition
TrapsReceived Count	Integer	Counter, number of traps received from the Audio Codes Server(s) during the collection period
TrapsFowarded Count	Integer	Counter, number of traps (from the Audio Codes Server(s)) forwarded/sent to the OAM framework during the collection period
UnknownTraps Count	Integer	Counter, number of traps received from an Unknown source during the collection period

The SysMgr component monitors all servers running Sun Solaris for the OM listed in the following table. These server OMs are viewed as part of the SysMgr's OM groups.

Each server's OMs are identified by the configured site and server name. For example, the OM group for a server in the Management Site with the configured name App1 will appear as MgmtSite App1.

Table 6 <SiteName> <ServerName>

OM Name	Format	Definition
CpuX_Util	0-100%	Percentage of time the CPU is busy, where X corresponds to the particular CPU on the server.
MemoryUtilization	0-100%	Percentage of memory utilized on the server.

Table 6 <SiteName> <ServerName>

OM Name	Format	Definition
Disk_Partition /x	0-100%	Percentage of disk space utilized for partition X. Each partition on the server is monitored for utilization. For example, percentage of disk space utilized for the partition /Var
INTF_X	0-100%	Percentage of bandwidth used on interface X, where X corresponds to a particular interface on the server.
SystemUptimeInHrs	Integer	Amount of time (in hours) the system has been up since its last reboot.

Security and administration

Topics in this chapter

Security

The Management Module operates within the protected CVoIP network, isolated from public network security risks. System access is the primary security risk to the Management Module and hosting servers. Access to both are password protected. Access needs to be limited to trusted administrative personnel.

Administrators may need to log onto the server(s) hosting the Management Module software to perform a manual failover procedure. The login requires the use of the password ‘sysadmin’ and the physical IP address of the server.

To prevent non-trusted employees from logging into the servers, it is recommended that both the password and server’s IP address remain confidential.

SNMP community string values for a server can be changed from the default ‘public’ to some other value for network security reasons. Once configured for a server, it applies this community string value to SNMP message traffic of the hosted components. Information on configuring the community string is documented in the *CVoIP System Management Console User Guide*.

Administration

The Management Module utilizes software pools to determine the versions of software that are available for use. Software pools are added onto the server hosting the Management Module via the Distributed Software Management (DSM). When an administrator

performs an add or update task from the System Management Console, the Management Module accesses the installed software pools and generates the loadlist displayed in the System Management Console.

To free up disk space on the server, administrators with the appropriate privileges can remove old and unused software versions by removing the associated pool from DSM. The procedure for removing a DSM pool is described in the procedure Removing software loads from the DSM pool.

Server backups

Backups of CVoIP servers allow recovery from a catastrophic hardware failure where a complete restore of the server's software (both third party and component software) is required. Backups of the Management Module hosting servers are recommended after third party software updates, such as an applied OS patch, and after maintenance release installations.

Removing software loads from the DSM pool

ATTENTION
The following procedure requires root access privileges to the server. Contact your next level of support if you need to perform this task and do not have the required server access.

In a network with redundant instances of the Management Module, the software pools are present on both servers hosting the Management Module. Perform the software removal on both servers to fully remove the older versions.

From an administrator workstation

1 Log onto the server hosting the Management Module.

2 List all the software pools that have installed on the system.

```
dsmlistpools
```

3 From the list, determine the pools that are not in use and can be safely removed.

4 Remove the software pool from the DSM load list. This command removes the load from the DSM pool, but does not delete the files from the file system. After this command has been executed, the component software associated with this pool will not appear in the System Management Console's load list window.

```
dsmdroppool <poolname>
```

where,
<poolname> identifies the software load being removed from the pool, for example ims_2.0_build195.

5

CAUTION

The following steps delete all the files from the directory where you execute the **rm -rf** command. Ensure you are in the correct directory before executing the command.

To delete the files of the software load from the file system, perform the following commands.

a Navigate to the directory of the removed software load.

```
cd <poolname>
```

where,
<poolname> is the directory name of the software load.

b Ensure you are in the correct directory by repeating the cd command.

```
cd <poolname>
```

c Only the user who owns the directory and files has permission to successfully delete them. Confirm you are the owner of the directory and files.

```
ls -l
```

If you are not listed as the owner of the directory and files, then you will have to login as the file owner. If you need to re-login, perform steps **a** and **b** again.

d Delete all the files in the directory.

```
/bin/rm -rf
```

e Navigate up to the parent directory of the software load directory.

```
cd ..
```

f Remove the empty directory from the file system.

```
rmdir <poolname>
```

6 Log off the server.

Succession

Carrier Voice over IP

Management Module Basics

Publication number: NN10369-111
Product release: (I)SN07
Document version: Standard 02.02
Date: December 2004

NORTEL NETWORKS™