ERICSSON

ENM System Administrator Guide

Operating Instructions

1/1543-AOM 901 151 Uen EN

Contents

1 ENM System Administrator Guide

This document provides the following information:

— Overview of all the ENM system-level administration tasks (indicating why and how frequently you need to perform a task).

— Detailed procedures for performing ENM system-level administration tasks.

— Any topics applicable to ENM on Cloud deployments are also applicable to Small Integrated ENM deployments.

— For detailed information on performing platform administration tasks for a Small Integrated ENM deployment refer to the Small Integrated ENM System Administration Guide- 1/1543 CAN 403 3456 [30].

For detailed information on performing ENM configuration, monitoring, or performance application administration tasks refer to the following documents:

— ENM Configuration System Administrator Guide

— ENM Monitoring System Administrator Guide

— ENM Performance System Administrator Guide

ENM performance and stability depend on having access to all resources from the specified hardware. If any other processes or activities are executed on this hardware, this can incur in adverse effects on system behavior and capability, therefore, it is done at customers own risk.

Additionally, in the case of a Customer Support Request (CSR) or fault report, Ericsson reserve the right to request to have any additional (non-Ericsson) functions disabled before Ericsson can do full analysis or troubleshooting of issue. Furthermore, this document describes configuration of a number of supported parameter, Ericsson does not support scenarios resulting from unauthorized configuration of unsupported parameters. The maintenance of hardware equipment is not described in this document. Refer to the Manufacturer's Manuals for hardware maintenance instructions.

Target Group

System Administrators.

2 Connect to a Service

2.1 Connect to a Virtual Machine on a Physical ENM Deployment

Prerequisites

A command window is open and you have `superuser` privileges.

Steps

1. Log on to the ENM MS as **`litp-admin`** user and switch to the **`root`** user.
2. List the contents of the host file to view all connected VMs within the deployment.

```
[root@ms-1 ~]# cat /etc/hosts
...
192.168.99.20 svc-1-pmserv # Created by LITP. Please do not edit
192.168.99.26 svc-1-netex # Created by LITP. Please do not edit
192.168.99.16 svc-1-ebc # Created by LITP. Please do not edit
192.168.99.36 svc-1-mspm # Created by LITP. Please do not edit
192.168.99.28 svc-1-uiserv # Created by LITP. Please do not edit
192.168.99.14 svc-1-supervc # Created by LITP. Please do not edit
..
192.168.99.32 svc-1-mscm # Created by LITP. Please do not edit
..
192.168.99.50 svc-1-jms # Created by LITP. Please do not edit
..
192.168.99.3 logstash # Created by LITP. Please do not edit
..
192.168.99.2 httpd # Created by LITP. Please do not edit
192.168.99.40 sso # Created by LITP. Please do not edit
..
192.168.99.12 svc-1-medrout # Created by LITP. Please do not edit
192.168.99.22 svc-1-cmserv # Created by LITP. Please do not edit
192.168.99.52 svc-1-sec # Created by LITP. Please do not edit
192.168.99.8 openidm # Created by LITP. Please do not edit
```

   The aliases for the parallel VMs take the form of `<SVC host>-<service>`.

   For example: `svc-1-cmserv, svc-2-cmserv`.

   The active-passive VMs take the form of `<service>`.

   For example: `httpd, sso, openidm`.

3. To access the VM, copy the private key of the cloud-user from its secure location to the `MS` or `SVC` node.

```
[root@ms-1 ~]# /root/.ssh/vm_private_key
```

Refer to *VM Security Tasks* in the *ENM System Administrator Guide* to learn more about the `vm_private_key`.

4. Connect by `SSH` to the VM you want.

   To access the `VM`, use the `cloud-user` user ID and include the path to the `VM` private key. For example:

```
[root@ms-1 ~]# ssh -i /root/.ssh/vm_private_key cloud-user@svc-1-cmserv
Last login: Thu Feb 26 10:14:43 2015 from 192.110.0.59
[cloud-user@svc-1-cmserv ~]# sudo su - root
[root@svc-1-cmserv ~]#
```

2.1.1 Connect to each ENM Physical Node

Prerequisites

— The root password was changed during the installation process and must be known by the system administrator. This must be repeated on all newly deployed ENM nodes.

— A command window is open.

Steps

1. Log on to each physical node from the MS

```
[root@ms-1 ~]$ ssh litp-admin@<node_hostname>
litp-admin@<node_hostname>'s password:
Last login: Mon Feb 23 11:25:13 2015 from ms-1
[litp-admin@<node_hostname> ~]$ su - root
Password:
[root@<node_hostname> ~]#
```

Note: Once connected, after the initial deployment, the passwords for both the `litp-admin` and `root` users must be changed.

2.2 Connect to a Virtual Machine on an ENM on Cloud Deployment

Prerequisites

— A command window is open and you have `superuser` privileges.

— You have access to the private key file for authentication, contact your OpenStack administrator

Steps

1. List the virtual machine aliases from the consul service:

   Using the private key for authentication, copy the key to the EMP server. Log on to EMP server and list the consul members to view all connected VMs within the deployment:

```
> scp -i <cloud-user private key> <cloud-user private key> cloud-user@<EMP I →
P Address>:/var/tmp/vm_private_key
> ssh -i <cloud-user private key> cloud-user@<EMP IP Address>
[cloud-user@ostk003-emp-0 ~]$ chmod 700 /var/tmp/vm_private_key
[cloud-user@ostk003-emp-0 ~]$ sudo su -
[root@ostk003-emp-0 ~]# consul members
Node                       Address          Status  Type    Build  Protocol  →
 DC
haproxy                    10.3.2.31:8301   alive   client  0.8.1  2         →
 dc1
opendj-1                   10.3.2.83:8301   alive   client  0.8.1  2         →
 dc1
opendj-2                   10.3.2.84:8301   alive   client  0.8.1  2         →
 dc1
openidm                    10.3.2.85:8301   alive   client  0.8.1  2         →
 dc1
ostk003-accesscontrol-0    10.3.1.251:8301  alive   client  0.8.1  2         →
 dc1
ostk003-accesscontrol-1    10.3.1.252:8301  alive   client  0.8.1  2         →
 dc1
ostk003-elasticsearch-0    10.3.2.15:8301   alive   client  0.8.1  2         →
 dc1
...
ostk003-neo4j-2            10.3.2.77:8301   alive   client  0.8.1  2         →
 dc1
ostk003-nfscommon-0        10.3.0.81:8301   alive   client  0.8.1  2         →
 dc1
ostk003-nfsnrbk-0          10.3.0.83:8301   alive   client  0.8.1  2         →
 dc1
ostk003-nfspm-0            10.3.0.85:8301   alive   client  0.8.1  2         →
 dc1
ostk003-nfspm-1            10.3.0.82:8301   alive   client  0.8.1  2         →
 dc1
...
ostk003-secserv-1          10.3.2.98:8301   alive   client  0.8.1  2         →
 dc1
ostk003-serviceregistry-0  10.3.2.100:8301  alive   server  0.8.1  2         →
 dc1
ostk003-serviceregistry-1  10.3.2.101:8301  alive   server  0.8.1  2         →
 dc1
ostk003-serviceregistry-2  10.3.2.102:8301  alive   server  0.8.1  2         →
 dc1
ostk003-uiserv-0           10.3.2.116:8301  alive   client  0.8.1  2         →
 dc1
ostk003-uiserv-1           10.3.2.117:8301  alive   client  0.8.1  2         →
 dc1
ostk003-vnflaf-services    10.3.1.249:8301  alive   client  0.8.1  2         →
 dc1
...
svc-2-httpd                10.3.2.35:8301   alive   client  0.8.1  2         →
 dc1
svc-2-sps                  10.3.2.111:8301  alive   client  0.8.1  2         →
 dc1
svc-2-sso                  10.3.2.113:8301  alive   client  0.8.1  2         →
 dc1
```

2. SSH to the VM you want.

   To access the VM, use the cloud-user user ID and include the path to the VM private key. The VM can be accessed using either the node identifier or it's IP address. For example:

```
[cloud-user@ostk003-emp-0 ~]$ ssh -i /var/tmp/vm_private_key cloud-user@10.3 →
.2.31
The authenticity of host 'haproxy (10.3.2.31)' can't be established.
RSA key fingerprint is b9:4f:ca:4f:bc:55:00:de:a8:77:e5:08:56:7c:db:98.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'haproxy,10.3.2.31' (RSA) to the list of known ho →
sts.
[cloud-user@haproxy ~]$
```

2.3 View Log Files and Dump Locations on a Virtual Machine

The following are details of log files available within each service in ENM.

Logs

All logs are configured to be forwarded to the Central Log Service. As such they are visible in Log Viewer using the ENM Launcher.

JBOSS Logs

All JBOSS logs are stored locally in `/ericsson/3pp/jboss/standalone/log`

3PP & System Logs

As standard, most 3PP and system logs are available locally in `/var/log`

Dumps

All application memory and core dump files are located in `/ericsson/enm/dumps`

3 Restarting a Service

3.1 Restart a Service on a Physical ENM Deployment

Prerequisites

— Root access to MS.

Steps

1. Establish the service instances installed on the ENM deployment using `grep` for a particular service instance:

```
[root@<MS> ~]# /opt/ericsson/enminst/bin/vcs.bsh --groups | grep <service_name>
```

Example

```
[root@ieatlms4352 ~]#  /opt/ericsson/enminst/bin/vcs.bsh --groups | grep msp
m

svc_cluster Grp_CS_svc_cluster_mspm ieatrcxb2539-1 parallel vm ONLINE OK -
svc_cluster Grp_CS_svc_cluster_mspm ieatrcxb4373    parallel vm ONLINE OK -
svc_cluster Grp_CS_svc_cluster_mspm ieatrcxb4374    parallel vm ONLINE OK -
```

2. Restart the VCS service group:

```
/opt/ericsson/enminst/bin/vcs.bsh --restart -g <service_group> -s <system>
```

Note: The `-s` command restarts only one service at a time. To restart multiple services, repeat the command and modify the system name.

It is not recommended (unless specifically instructed) to restart more than one instance of a service at the same time. Restarting more than one instance of a service at the same time impacts the service availability and also results in some application specific consequences.

Example

```
/opt/ericsson/enminst/bin/vcs.bsh --restart -g Grp_CS_svc_cluster_mspm -s ieatrcxb4373

[root@ms-1 bin]# bash vcs.bsh --restart -g Grp_CS_svc_cluster_mspm -s ieatrcxb4373
2020-07-23 12:02:04.481 INFO hagrp_offline : Offlining 1 group(s)
2020-07-23 12:02:04.515 INFO hagrp_offline : Offlining Grp_CS_svc_cluster_mspm on ieatrcxb4373
2020-07-23 12:02:04.807 INFO wait_vcs_state : Waiting for Grp_CS_svc_cluster_mspm to go OFFLINE on ieatrcxb4373 (timeout=1800)
2020-07-23 12:05:43.185 INFO wait_vcs_state : Group Grp_CS_svc_cluster_mspm now OFFLINE on ieatrcxb4373 (3m:39s)
```

```
2020-07-23 12:05:43.817 INFO hagrp_online : Onlining 1 group(s)
2020-07-23 12:05:43.822 INFO online_services : Onlining Grp_CS_svc_cluster_m
spm on ieatrcxb4373
2020-07-23 12:05:44.057 INFO wait_vcs_state : Waiting for Grp_CS_svc_cluster
_mspm to go ONLINE on ieatrcxb4373 (timeout=4500)
2020-07-23 12:09:03.400 INFO wait_vcs_state : Group Grp_CS_svc_cluster_mspm
now ONLINE on ieatrcxb4373 (3m:19s)
[root@ms-1 bin]#
```

3. Verify if the service instance is `ONLINE`:

```
/opt/ericsson/enminst/bin/vcs.bsh --groups | grep mspm
```

Example

```
[root@ieatlms4352 ~]#  /opt/ericsson/enminst/bin/vcs.bsh --groups | grep msp
m

svc_cluster Grp_CS_svc_cluster_mspm ieatrcxb2539-1 parallel vm ONLINE OK -
svc_cluster Grp_CS_svc_cluster_mspm ieatrcxb4373    parallel vm ONLINE OK -
svc_cluster Grp_CS_svc_cluster_mspm ieatrcxb4374    parallel vm ONLINE OK -
```

4. After the service restarted in *Step 2* is `ONLINE`, you can repeat *Step 2* and *Step 3* to restart further instances of the service as per your requirement.

3.2 Restart a Service on an ENM on Cloud Deployment

Prerequisites

— User connected to EMP server.

Steps

1. Establish the service instances installed on the vENM deployment using grep for a particular service instance.

```
#consul members | grep <service name>
```

Example

```
#consul members | grep mscm
```

2. Connect to the VM of the service group by following *section 3.2* and trigger a healthcheck failure of the VM by killing consul.

```
#pkill consul
```

3. Verify if the service instance is ONLINE.

4. After the restarted service is ONLINE, repeat the preceding two steps to restart further instances of the service as per your requirement.

4 Configuring PIB Parameters

> To configure a Platform Integration Bridge (PIB) parameter, it is necessary to determine what environment you are working on and follow the task relevant to your environment.

4.1 Configuring PIB Parameters on a Physical ENM Deployment

To access the PIB (Platform Integration Bridge) script to update parameters for ENM applications, it is necessary to determine what environment you are working on and follow the task relevant to your environment. This task outlines the steps to read and configure PIB parameters on a physical ENM Deployment.

Prerequisites

- A command window is open and you have super user privileges.
- You are connected to the ENM MS as per the Connect to a Virtual Machine on a Physical ENM Deployment on page 2.

Steps

1. Find the hostname for the service instance:

   ```
   grep <service_name> /etc/hosts
   ```

2. Choose one of the returned hostnames for the next steps.
3. Navigate to the following directory:

   ```
   [root @ms-1 ~]# cd /ericsson/pib-scripts/etc/
   ```

4. Check a configuration parameter on sample VM:

   ```
   ./config.py read --app_server_address=<service VM hostname>:8080 --service_i →
   dentifier=<service_identifier_name> --name=<parameter_name>
   ```

   Note: `--service_identifier=<service_identifier_name>` is optional for this command.

   Example

   To check value of the `SMRS_ERBS_NoOf_BACKUP_FILES` parameter:

```
./config.py read --app_server_address=svc-1-smrsserv:8080 --name=SMRS_ERBS_N
oOf_BACKUP_FILES
```

5. Update a configuration parameter on a deployed VM:

```
./config.py update --app_server_address=<service VM hostname>:8080 --service
_identifier=<service_identifier_name> --name=<parameter_name> --value=<new_v
alue>
```

Note: `--service_identifier=<service_identifier_name>` is optional for this command.

Example

To update the `SMRS_ERBS_NoOf_BACKUP_FILES` value to 4:

```
./config.py update --app_server_address=svc-1-smrsserv:8080 --name=SMRS_ERBS
_NoOf_BACKUP_FILES --value=4
```

Results

You have updated an application parameter using the PIB script.

4.2 Configuring PIB Parameters on ENM on Cloud Deployment

To access the PIB (Platform Integration Bridge) script to update parameters for ENM applications, it is necessary to determine what environment you are working on and follow the task relevant to your environment. This task outlines the steps to read and configure PIB parameters on an ENM on Cloud Deployment.

Note: ENM concepts are explained in the *ENM Product Description*.

Prerequisites

— A command window is open and you have super user privileges.

— You are connected to an EMP VM using Connect to a Virtual Machine on an ENM on Cloud Deployment on page 3.

Steps

1. As cloud-user change to root:

```
[cloud-user@emp ~]$ sudo su -
[root@emp ~]#
```

2. Find the hostname for the service instance:

```
consul members|grep <service_name>
```

3. Choose one of the returned hostnames for the next steps.
4. Change directory to where the config.py script is located:

```
[root@emp ~]# cd /ericsson/pib-scripts/etc/
[root@gat-emp-0 etc]#
```

5. Read the current parameter value:

```
./config.py read --app_server_address=<service VM hostname>:8080 --service_i →
dentifier=<service_identifier_name> --name=<parameter_name>
```

6. Set the parameter to the required value:

```
./config.py update --app_server_address=<service VM hostname>:8080 --service →
_identifier=<service_identifier_name> --name=<parameter_name> --value=<new_v →
alue>
```

Results

You have updated an application parameter using the PIB script.

5 System Level Maintenance Tasks for LITP based Deployments

5.1 ENM System Health Check

This script is executed from the ENM Management Server, and the results provide information on the state of various aspects of an ENM deployment. Checks include:

— All servers in the clusters are available and running.

— ENM applications and services are available and online.

— Filesystem usage on the servers is not exceeding critical levels.

— PostgreSQL Database Administrator Password expiration status.

Key system level services are running (for example: `sshd`, `puppet`, `vcs`, `rhq-agent`, `litpd`, `ddc`, `mcollective`)

This script is run after an ENM Installation, Upgrade, or Restore from Backup procedure has occurred. However, it can be run at any point in time, to determine the health of the ENM system.

Prerequisites

— ENM has been deployed.

— User has root access to the ENM Management Server

Steps

1. Log on to the ENM MS as the litp-admin user, then switch to the root user:

   If password authentication is disabled for the litp-admin user, then refer to *Log on to the MS When Password Authentication is Disabled* in the *LITP Node Hardening Instructions*.

   Command Syntax:

   ```
   # ssh litp-admin@<Management Server>
   # su -
   ```

   Example

   ```
   #ssh root@10.10.10.10
   ```

Result:

```
############  WARNING ############

This system is
for authorised use only. By using this system you consent to monitoring and
data collection.
#################################
root@10.10.10.10's
password:
Last login: Fri
Aug 25 12:12:06 2017 from server.example.com
[root@ms-1~]#
```

2. Enter the command to execute the ENM System Healthcheck script:

   Command Syntax:

   ```
   /opt/ericsson/enminst/bin/enm_healthcheck.sh [--verbose]
   ```

   Example

   ```
   /opt/ericsson/enminst/bin/enm_healthcheck.sh [--verbose]
   ```

   Note: Executing the script with the "-h" option will display the full usage of the script.

   Result:

   ```

   ```

   Command Result:

   ```
   Note: If the healthcheck script reports any errors contact Ericsson Customer →
    Support.

   Beginning ENM pre-Healthchecks
   Node Status: PASSED
   Completed ENM pre-Healthchecks
   Beginning ENM System Healthcheck
   ------------------------------------------------------------------
   ...
   ...
   ...
   ------------------------------------------------------------------
   Successfully Completed ENM System Healthcheck
   ------------------------------------------------------------------
   [root@ms-1~]#
   ```

5.2 ENM FCAPS Health Check

This script is executed from the ENM Management Server, and the results provide information about various FCAPS aspects of the ENM Deployment. Checks include:

— Total number of nodes managed by the ENM, per node type

— Total number of FM synced nodes per node type

— Total number of CM synced nodes per node type

— Total number of SHM synced nodes per node type

— Total number of PM synced nodes per node type

— Number of PM files received for the last hour

The unsynced node list can be found in `/var/log/report/<node_name>`, with filename `unsynced_<NETYPE>.txt.<timestamp>` where *<node_name>* can be FM, CM, SHM, or PM.

Example:

```
#ls -ltr /var/log/reports/FM/
total 20
-rw-r--r--. 1 root root 15890 Oct  5 15:17 unsynched_ERBS.txt.201810051516
-rw-r--r--. 1 root root    18 Oct  5 15:17 unsynched_RadioNode.txt.201810051516
```

This script can be run before or after an ENM upgrade. Execution of the script during ENM Upgrade is not supported. However, it can be run at any point in time, outside of ENM Upgrade, to determine the FCAPS healthcheck summary of the ENM system.

Prerequisites

— ENM has been deployed.

— User has `root` access to the ENM Management Server.

— ENM user has at least `Cmedit_Operator` and `PM_NBI_Operator roles`.

Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. Enter the command to execute the ENM FCAPS health check summary script:

   ```
   /opt/ericsson/enminst/bin/enm_healthcheck.sh --action fcaps_healthcheck [--v →
   erbose]
   ```

   If the script is executed with the `--verbose` option, a more detailed output is displayed.
3. Enter the username and password for the ENM `administrator` user.

   ```
   Beginning ENM pre-Healthchecks
   Node Status: PASSED
   Completed ENM pre-Healthchecks
   Checking FCAPS Summary per Node Types:
   Enter ENM user to check FCAPS:administrator
   ```

```
Enter administrator password:
Fetching the number of synced/unsynced nodes:
NeType              # of Nodes    FM Synced CM Synced SHM Synced PM Synced P →
M Files/hr(2018-10-05'T'14:00:00-2018-10-05'T'15:00:00)
ERBS                17454        16985     17288     17279      17454         →
   69124
RadioNode       2259          2258        2259          478         2259      →
      14557
Unsynched nodes list can be found in /var/log/reports
[root@ms-1~]#
```

If the health check script reports any errors contact Ericsson Customer Support.

5.3 VM Security Tasks

After an initial installation or upgrade, you must execute these tasks to secure the `vm_private_key`, which is used for Virtual Machine (VM) connectivity.

The `vm_private_key` is generated automatically during an initial installation, or upgrade, if the `--regenerate_keys` option is passed. It is stored on the LMS (see layout diagram in the *ENM Product Description*).

Note: Connection to each VM is permitted only through `cloud-user`. The `cloud-user` is a password-less system user, that works with the `vm_private_key`.

The `vm_private_key` is available under the following path: `# /root/.ssh/vm_private_key`

Note: It is highly recommended that you store the `vm_private_key` in a secure location off the system, and only copy it back when VM access is necessary.

Prerequisites

— Initial installation or upgrade was completed successfully.

Steps

1. Log on to the ENM MS as the `litp-admin` user, then switch to the root user.
2. Locate the `vm_private_key`:

   ```
   [root@ms-1 ~]# ls /root/.ssh/vm_private_key
   ```

3. Move the `vm_private_key` from the LMS and store it in a secure location away from the deployment.

Results

VM access is restricted to the `cloud-user` ID using the `vm_private_key`.

5.3.1 Regenerating SSH Keys

If the `vm_private_key` becomes lost or misplaced, VMs will not be accessible.

Note: Regenerating the VM private key creates a plan that rolls over all nodes (except the DBs) and may take between 60 and 180 minutes to complete, depending on the size of the deployment. Once regenerated, the previous `vm_private_key` is invalid.

Steps

1. Log on to the ENM MS as the litp-admin user, then switch to the root user.
2. Execute the enminst_healthcheck script to ensure the system is in a healthy state.
3. Take a snapshot of the system.

   To do this, follow the steps outlined in the chapter *Snapshot the System* in the page 354.
4. Regenerate the SSH keys.

   To regenerate the `vm_private_key`, execute the following commands:

   ```
   [root@ms-1 ~]# cd /opt/ericsson/enminst/bin
   [root@ms-1 bin]# bash ssh_key_creation.sh --regenerate
   ```

   Note: If an issue occurs during the regeneration of SSH keys, follow the steps in the *Rollback Procedure* section in the page 354 to bring the system back to an OK state.
5. Once completed successfully, locate the `vm_private_key`:

   ```
   [root@ms-1 ~]# ls /root/.ssh/vm_private_key
   ```
6. Move the `vm_private_key` from the LMS and store it in a secure location away from the deployment.
7. Remove the snapshots.

   To do this, follow the steps outlined in the section *Remove the Snapshots* in page 354.

5.4 Change litp-admin and root User Passwords

After connecting to each physical node, it is possible to change the passwords for the root user, the litp-admin user, or both. Do not change these passwords during a backup, a restore of the ENM deployment, or during an ENM upgrade. If you restore from a backup that was taken before changing passwords, the restored

backup requires the original passwords. For information about setting passwords, refer to *Password Handling* in the *ENM ENM Identity and Access Management System Administrator Guide* (2/1543-AOM 901 151-1 Uen).

Steps

1. Log on to the ENM MS as the litp-admin user, then switch to the root user.
2. Change the password for the root user:

```
[root@ms-1~]# passwd
Changing password for user root.
New password:
Retype newpassword:
passwd: all authentication tokens updated successfully.
```

3. Change the password for the litp-admin user:

```
[root@ms-1~]# passwd litp-admin
Changing password for user litp-admin.
New password:
Retype newpassword:
passwd: all authentication tokens updated successfully.
[root@ms-1~]#
```

4. Check if the `/home/litp-admin/.litprc` file exists.

   If so, edit the file to ensure that the password value for litp-client matches the new password for the litp-admin user. Alternatively, remove the .litprc files as described in *Enable Local Trust Authentication for Existing Users*.

5. Log on to each peer server as the litp-admin user and change the password:

```
[root@ms-1~]# ssh litp-admin@svc-1
[litp-admin@svc-1~]$ passwd
Changing password for user litp-admin.
Changing password for litp-admin.
(current) UNIX password:
New password:
Retype newpassword:
passwd: all authentication tokens updated successfully.
```

6. Switch to the root user on each peer server and change the password:

```
[litp-admin@svc-1~]$ su
Password:
[root@svc-1 litp-admin]# passwd
Changing password for user root.
New password:
Retype newpassword:
passwd: all authentication tokens updated successfully.
```

5.5 Change es_admin User Password

The default password for the `es_admin user` at initial ENM deployment is EsUser123. This task can be used to change the password.

Steps

1. Log on to the ENM MS as the root user.
2. Change the password for the `es_admin` user:

```
[root@ms-1~]# passwd es_admin
Changing password for user es_admin.
New password:
Retype newpassword:
passwd: all authentication tokens updated successfully.
```

5.6 Check LITP Component Certificate Expiry Date

The following LITP component certificates have a validity time period. Check the expiry date of the installed certificate.

— Puppet (5 years)

— PuppetDB (5 years)

— RabbitMQ (5 years)

— MCollective (5 years)

Puppet CA signs the certificates of Puppet, PuppetDB, RabbitMQ, and MCollective.

If the certificates have an expiry date within the next year, then they must be extended.

Prerequisites

— User has root access to the ENM Management Server.

Steps

1. Log on to the ENM MS as the litp-admin user and switch to the root user.
2. Check the expiry date of the Puppet certificate.

```
[root@ms1 ~]# openssl x509 -enddate -noout -in /var/lib/puppet/ssl/certs/ca.
pem
notAfter=Dec 26 14:21:15 2023 GMT
```

3. Extend the expiry date for any of the components that expire within the next 12 months.

   For more information, see Extend LITP Component Certificate Expiry Date on page 18.

5.7 Extend LITP Component Certificate Expiry Date

The following LITP component certificates have a validity time period. Extend the expiry date of the installed certificate if they expire within the next 12 months.

— Puppet (5 years)

— PuppetDB (5 years)

— RabbitMQ (5 years)

— MCollective (5 years)

Prerequisites

— User has root access to the ENM Management Server and Peer Servers.

Steps

1. Log on to the ENM MS as the litp-admin user and switch to the root user.
2. Extend the expiry date of the Puppet certificate. Extending the Puppet CA certificate also automatically extends the RabbitMQ and MCollective certificate expiry dates.

   a. Remove the existing certificate.

   ```
   [root@ms1 ~]# rm -rf /var/lib/puppet/ssl
   ```

   b. Generate a new certificate for the CA.

   ```
   [root@ms1 ~]# puppet cert --generate $(puppet master --configprint
   certname)
   ```

3. Extend the expiry date of the PuppetDB certificate.

   a. Remove the old PuppetDB certificates.

   ```
   [root@ms1 ~]# rm -rf /etc/puppetdb/ssl/
   ```

   b. Generate a new PuppetDB certificate.

```
[root@ms1 ~]# puppetdb ssl-setup
```

c. Restart the PuppetDB service.

```
[root@ms1 ~]# service puppetdb restart
```

d. Restart the Puppet Server.

```
[root@ms1 ~]# service puppetserver restart
```

4. Restart Puppet service.

```
[root@ms1 ~]# service puppet restart
```

5. Generate new certificates on all the peer servers.

   a. Log on to each peer server as the litp-admin user and switch to the root user.

   b. Delete the certification on the peer servers.

```
[root@node1 ~]# rm -rf /var/lib/puppet/ssl
```

   c. Restart puppet on peer servers.

```
[root@node1 ~]# service puppet restart
```

   Repeat this step for all peer servers in the deployment. For peer servers that are offline ensure that the certificates are generated when they come back online.

5.8 Enable Local Trust Authentication for Existing Users

LITP provides several options for REST interface authentication. The local trust authentication option provides authentication (based on the user who is currently logged in over the UNIX socket protocol) without requiring password credentials.

Prerequisites

— The ENM upgrade has completed successfully.

— You have logged off from all sessions as the litp-admin user.

— You have previously created .litprc files during an install procedure. Check if these files exist by running the following command:

```
[root@ms]# ls /home/litp-admin/.litprc
/home/litp-admin/.litprc
[root@ms]# ls /root/.litprc
/root/.litprc
```

Steps

1. Add the user to the UNIX socket group for LITP trust authentication.

   ```
   [root@ms]# usermod -a -G litp-access litp-admin
   ```

2. Delete the .litprc files.

   ```
   [root@ms]# rm /home/litp-admin/.litprc
   [root@ms]# rm /root/.litprc
   ```

3. Verify that you can issue LITP commands by running the following litp version command.

   The output is similar to the following example:

   ```
   [root@ms]# litp version
   LITP2 1.46.2 CXP9030418 R1AAG02
   ```

4. Verify that the litp-admin user is added to the litp-access group.

   ```
   [root@ms]# groups litp-admin
   litp-admin : litp-admin litp-access
   [root@ms]#
   ```

5.9 Check the Status of the OMBS Backups

This script is executed from the ENM Management Server, and the results provide information about OMBS backup verification.

Checks include:

— ENM version of the backup matches the current ENM version.

— Last backup date is not more than a week old.

This script is run before ENM upgrade or any significant change of the system is planned, to ensure that a valid backup is present. However, it can be run at any point in time, to determine the ENM OMBS backup validity.

Prerequisites

— ENM has been deployed.

— OMBS has been deployed.

— User has root access to the ENM Management Server.

— User has root access to OMBS server.

— The OMBS IP address is known.

Steps

1. Log on to the ENM MS as the litp-admin user, then switch to the root user.:

   If password authentication is disabled for the litp-admin user, then refer to *Log on to the MS When Password Authentication is Disabled* in the *LITP Node Hardening Instructions*.

   ```
   # ssh litp-admin@<Management Server>
   # su -
   ```

2. Enter the command to execute the ENM OMBS summary script:

   ```
   /opt/ericsson/enminst/bin/enm_healthcheck.sh --action ombs_backup_healthchec →
   k [--verbose]
   ```

   If the script is executed with the --verbose option, a more detailed output is displayed.

3. Enter the OMBS IP address:

   ```
   Enter OMBS IP Address:
   ```

4. Enter the OMBS root password:

   ```
   Enter OMBS root pass:
   ```

   Example:

   ```
   Beginning ENM pre-Healthchecks
   Node Status: PASSED
   Completed ENM pre-Healthchecks
   OMBS Backup Verification:
   Enter OMBS IP Address:10.32.210.220
   Enter OMBS root pass:
   This may take some time. Please wait..
   ------------------------------------------------------------------------
   SNo. ENM_Version Start_Time Expiry_Time Keyword
   ------------------------------------------------------------------------
   1 ENM 19.01 2019-02-16 00:08:25 2019-03-19 00:08:25 ENM_iegtlms11-bkp_201902 →
   16000020
   2 ENM 19.01 2019-02-14 00:08:06 2019-03-17 00:08:06 ENM_iegtlms11-bkp_201902 →
   14000020
   ```

```
3 ENM 19.01 2019-02-13 12:05:05 2019-03-16 12:05:05 ENM_iegtlms11-bkp_201902 →
13115744

Last successful OMBS backup was taken on 2019-02-16
```

Note: If the health check script reports any errors contact Ericsson Customer Support.

5.10 ENM Power On Procedure

Use this procedure to power on each node within the ENM deployment. This procedure is executed from the ENM MS.

Prerequisites

— Root access to MS.

— Refer to the Site Engineering Document to obtain the `ilo` address, username, and password for each node in the ENM deployment.

Follow the sequence table order to power on clusters.

Table 1 Power On Sequence

Power On Sequence	Cluster Type
1.	db_cluster
2.	svc_cluster
3.	scp_cluster
4.	evt_cluster
5.	str_cluster
6.	ebs_cluster
7.	asr_cluster
8.	eba_cluster

Steps

1. Establish what clusters are installed on the ENM deployment:

```
[root@ms-1 ~]# cd /opt/ericsson/enminst/bin
[root@ms-1 bin]# bash vcs.bsh --systems
```

Sample Output:

```
[root@ms-1 bin]# bash vcs.bsh --systems
  ------------  -------  -----------  ------
        System    State      Cluster  Frozen
  ------------  -------  -----------  ------
         asr-1      N/A  asr_cluster       -
```

```
          scp-1      N/A  scp_cluster       -
          ebs-1      N/A  ebs_cluster       -
          str-1      N/A  str_cluster       -
          scv-1      N/A  svc_cluster       -
           db-1      N/A   db_cluster       -
  ------------  -------  -----------  ------
[root@ms-1 bin]#
```

Note: Warnings are displayed when all nodes in a cluster are powered down as the discovery mechanism can't ping the blade. These warnings can be safely ignored.

2. Based on the Power On sequence table, power on each node in the cluster by executing the following command:

```
curl -s -L -k --user <user:password> -H "Content-Type: application/json" -d
'{"ResetType": "On"}' -X POST https://<ip-address>/redfish/v1/Systems/1/Acti
ons/ComputerSystem.Reset
```

3. Ensure that the node is powered on:

```
curl -s -L -k --user <user:password> -X GET https://<ip-address>/redfish/v1/
Systems/1 | egrep -o "PowerState.{1,7},"
```

4. Wait for `mco` to find the host-names of the cluster.

```
root@ms-1 ~]# mco ping
```

Note: Use the watch command to follow the `mco` ping on an interval

```
root@ms-1 ~]# watch -n 2 -d 'mco ping'
```

5. Ensure that the service groups are online.

```
root@ms-1 ~]# cd /opt/ericsson/enminst/bin
root@ms-1 ~]# bash vcs.bsh --groups -c <cluster name>
```

Note: The service groups are brought online automatically and may take a few minutes.

Example

```
root@LMS:~# vcs.bsh --groups -c db_cluster
Getting groups from cluster db_cluster on system ieatrcxb6205
---------- ------------------------------------------------- ------------
-------------- ----------- ------------ ---------- ------
Cluster Group System HAType ServiceType ServiceState GroupState Frozen
---------- ------------------------------------------------- ------------
-------------- ----------- ------------ ---------- ------
db_cluster Grp_CS_db_cluster_jms_clustered_service ieatrcxb6225 active-stand
by lsb OFFLINE OK -
db_cluster Grp_CS_db_cluster_jms_clustered_service ieatrcxb6305 active-stand
by lsb ONLINE OK -
db_cluster Grp_CS_db_cluster_modeldeployment_cluster_service_1 ieatrcxb6309
active-standby lsb ONLINE OK -
db_cluster Grp_CS_db_cluster_modeldeployment_cluster_service_1 ieatrcxb6205
active-standby lsb OFFLINE OK -
db_cluster Grp_CS_db_cluster_postgres_clustered_service ieatrcxb6225 active-
```

```
standby lsb ONLINE OK -
db_cluster Grp_CS_db_cluster_postgres_clustered_service ieatrcxb6305 active- →
standby lsb OFFLINE OK -
db_cluster Grp_CS_db_cluster_elasticsearch_clustered_service ieatrcxb6225 ac →
tive-standby lsb ONLINE OK -
db_cluster Grp_CS_db_cluster_elasticsearch_clustered_service ieatrcxb6305 ac →
tive-standby lsb OFFLINE OK -
db_cluster Grp_CS_db_cluster_opendj_clustered_service ieatrcxb6225 parallel  →
lsb ONLINE OK -
db_cluster Grp_CS_db_cluster_opendj_clustered_service ieatrcxb6305 parallel  →
lsb ONLINE OK -
db_cluster Grp_CS_db_cluster_sg_neo4j_clustered_service ieatrcxb6309 paralle →
l lsb ONLINE OK -
db_cluster Grp_CS_db_cluster_sg_neo4j_clustered_service ieatrcxb6305 paralle →
l lsb ONLINE OK -
db_cluster Grp_CS_db_cluster_sg_neo4j_clustered_service ieatrcxb6205 paralle →
l lsb ONLINE OK -
---------- ----------------------------------------------------- ------------  →
-------------- ----------- ------------ ---------- ------
```

6. Once the GroupState column is in a state of OK, as shown in the example, repeat steps 2–5 for the next cluster based on the sequence listed in the Power On Sequence table.

7. Once all the nodes are online and VCS service groups are OK on each node, execute the ENM health check script to ensure that the system is in the correct working order.

```
[root@ms-1 ~]# cd /opt/ericsson/enminst/bin
[root@ms-1 bin ]# bash enm_healthcheck.sh
```

5.11 ENM Power Down Procedure

Use this procedure to correctly shut down each node in the ENM deployment. This procedure is executed from the ENM MS.

Note: If all instances of uiserv are offline, some non-critical data will be lost.

The following UI settings will not be preserved if all instances of uiserv are powered down:

Table 2

Application	Settings
Application Launcher	Favorite applications
Alarm Monitor	Workspaces
Alarm Overview	Workspaces
Alarm Search	Workspaces
Network Explorer	Favorite collections, Favorite Saved Searches
Network Health Monitor	Workspaces
Node Monitor	Workspaces

Application	Settings
Log Viewer	Custom table columns
KPI Management	Custom table columns
Multi-Node Health Monitor	Custom table columns

Prerequisites

— Root access to MS.

— Refer to the Site Engineering Document to obtain the `ilo` address, username, and password for each node in the ENM deployment.

Steps

Follow the sequence table order to power down the clusters.

Table 3 Power Down Sequence

Power Down Sequence	Cluster Type
1.	asr_cluster
2.	ebs_cluster
3..	eba_cluster
4.	str_cluster
5.	evt_cluster
6.	scp_cluster
7.	svc_cluster
8.	db_cluster

1. Log on to the ENM MS as the litp-admin user, then switch to the root user.
2. Execute the ENM healthcheck to ensure that the system is in a healthy state:

```
[root@ms-1 ~]# cd /opt/ericsson/enminst/bin
[root@ms-1 bin ]# bash enm_healthcheck.sh --action vcs_service_group_healthc →
heck vcs_cluster_healthcheck
```

Result: Expected output should indicate that all tests have passed successfully:

```
[root@ms-1 bin ]# bash  /opt/ericsson/enminst/bin/enm_healthcheck.sh --actio →
n vcs_service_group_healthcheck vcs_cluster_healthcheck
Beginning ENM pre-Healthchecks
Node Status: PASSED
Completed ENM pre-Healthchecks
Beginning VCS Service Group Healthcheck
Successfully Completed VCS Service Group Healthcheck
Beginning VCS Cluster System Healthcheck
Successfully Completed VCS Cluster System Healthcheck
[root@ms-1 ~]#
```

3. Establish what clusters are installed on the ENM deployment.

```
[root@ms-1 ~]# cd /opt/ericsson/enminst/bin[root@ms-1 bin]# bash vcs.bsh --s →
ystems
```

Example output:

```
[root@ms-1 bin]# bash vcs.bsh --systems
------------  -------  -----------  ------
System    State      Cluster  Frozen
------------  -------  -----------  ------
esa-1        RUNNING  esa_cluster      -
str-1        RUNNING  str_cluster      -
evt-1        RUNNING  evt_cluster      -
scp-1        RUNNING  scp_cluster      -
svc-1        RUNNING  svc_cluster      -
db-1         RUNNING  db_cluster       -
------------  -------  -----------  ------
```

4. Based on the Power Down Sequence table, choose the cluster type to list all service groups.

```
[root@ms-1 bin]# bash vcs.bsh --groups -c <cluster name>
```

Example

```
[root@ma-1 bin]# bash vcs.bsh --groups -c scp_cluster
Getting groups from cluster scp_cluster on system ieatrcxb6022
-----------  ------------------------------------  ------------  --------   →
-----------  ------------  ----------  ------
Cluster                                  Group        System    HAType  Serv →
iceType  ServiceState  GroupState  Frozen
-----------  ------------------------------------  ------------  --------   →
-----------  ------------  ----------  ------
scp_cluster           Grp_CS_scp_cluster_scripting  scp-2            paralle →
l           vm        ONLINE          OK       -
scp_cluster           Grp_CS_scp_cluster_scripting  scp-1            paralle →
l           vm        ONLINE          OK       -
scp_cluster      Grp_CS_scp_cluster_elementmanager  scp-2            paralle →
l           vm        ONLINE          OK       -
scp_cluster      Grp_CS_scp_cluster_elementmanager  scp-1            paralle →
l           vm        ONLINE          OK       -
scp_cluster  Grp_CS_scp_cluster_scriptinglvsrouter  scp-2            paralle →
l           vm        ONLINE          OK       -
scp_cluster  Grp_CS_scp_cluster_scriptinglvsrouter  scp-1            paralle →
l           vm        ONLINE          OK       -
-----------  ------------------------------------  ------------  --------   →
-----------  ------------  ----------  ------
```

5. Offline all VCS service groups listed using the previous command, with the exception of `lvsrouter` group entries.

```
[root@ms-1 bin]# bash vcs.bsh --offline -g <service_group>
```

Example

```
[root@ms-1 bin]# bash vcs.bsh --offline -g Grp_CS_scp_cluster_scripting
2016-10-27 10:22:36 INFO  hagrp_offline                 : Offlining 1 group(s)
2016-10-27 10:22:36 INFO  hagrp_offline                 : Offlining Grp_CS_scp_cluster_scripting on scp-2
2016-10-27 10:22:36 INFO  wait_vcs_state                : Waiting for Grp_CS_scp_cluster_scripting to go OFFLINE on scp-2 (timeout=900)
2016-10-27 10:25:29 INFO  wait_vcs_state                : Group Grp_CS_scp_cluster_scripting now OFFLINE on scp-2 (2m:53s)[root@ms-1 bin]#
```

6. When all service groups are successfully offline in the cluster, then shut down the `lvsrouter` group entries for that cluster.

```
[root@ms-1 bin]# bash vcs.bsh --offline -g <lvsrouter_service_group> -s <system>
```

Once the service groups are successfully offline, repeat steps 3–5 for all clusters as listed in the Power Down Sequence table.

7. Power down all nodes in the clusters as listed in the Power Down Sequence table.

```
curl -s -L -k --user <user:password> -H "Content-Type: application/json" -d '{"ResetType": "ForceOff"}' -X POST https://<ip-address>/redfish/v1/Systems/1/Actions/ComputerSystem.Reset
```

8. Ensure that the nodes have successfully powered down by checking the status:

```
curl -s -L -k --user <user:password> -X GET https://<ip-address>/redfish/v1/Systems/1 | egrep -o "PowerState.{1,7},"
```

5.12 Launch Firefox Remotely from the Management Server

In certain circumstances, where troubleshooting or maintenance is required, you may need to remotely access the following management GUIs:

— EMC Unisphere

— HP Onboard Administrator

— HP iLO

— HP Virtual Connect Manager

Prerequisites

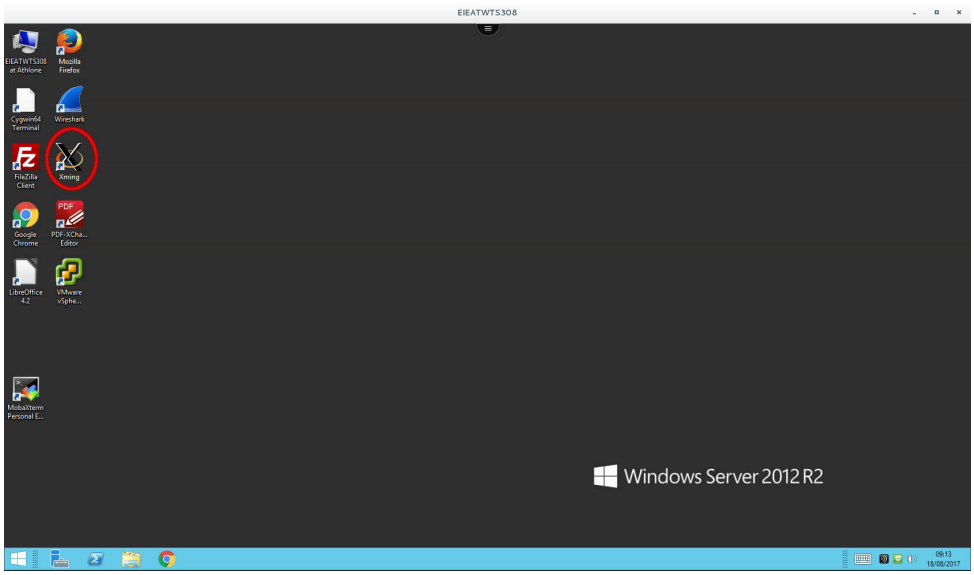
— SSH access to the Management Server.

— X Server software for Windows.

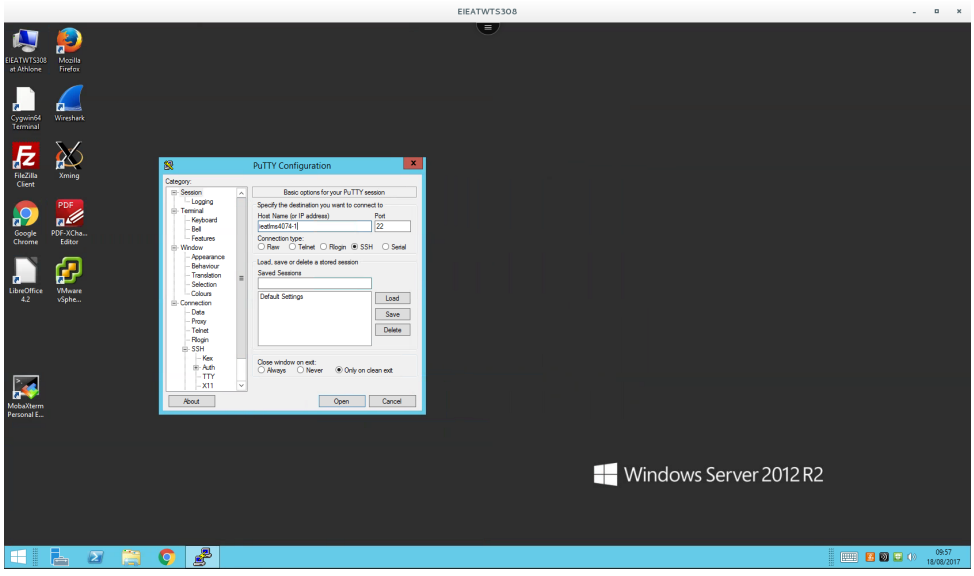
— An SSH client installed on the local Windows or Linux workstation, for example MobaXterm or PuTTY for Windows.

Steps

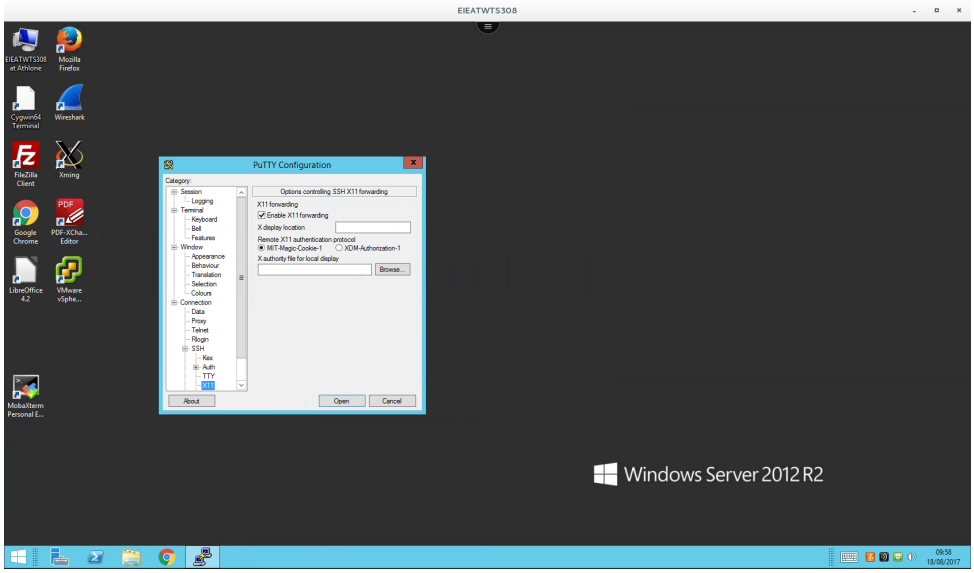
1. Download and install an X Server for Windows (for example Xming).
2. Launch the X Server:



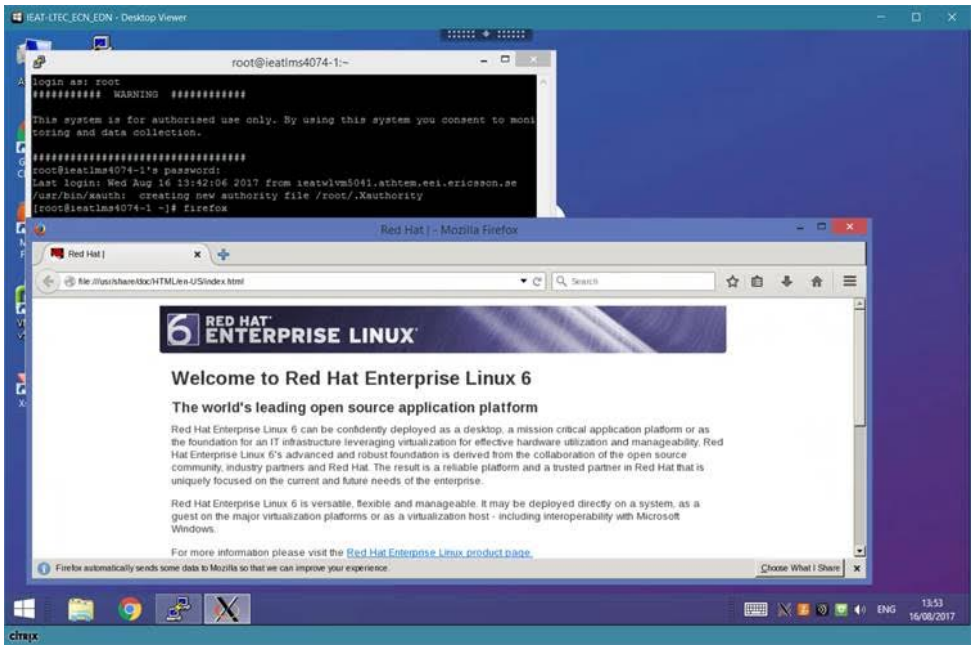
3. Download an SSH client, for example PuTTY.
4. Start an SSH client session to the Management Server:



5. Select Enable X11 forwarding and click **Open**:



6. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
7. Execute the `firefox` command. The Firefox browser is launched.



8. In the URL address bar, enter the IP address of the Management GUI that you need to access.

Note: Java based GUIs and Flash plugin GUIs (eg. HP Virtual Connect Manager) are not supported in Firefox versions later than Firefox 52 ESR and Firefox 68 ESR respectively.

To access a Java based GUI or Flash plugin based GUI via Firefox from the Management Server, temporarily downgrade to the original Firefox 52 version that is available on the RHEL6.10 ISO. This is not recommended as this older version of Firefox is now considered a security risk. Refer to *Accessing Java based GUIs and Flash plugins based GUIs using Firefox* in the ENM Troubleshooting Guide [19].

Results

Firefox browser is launched from the Management Server and you are able to access the management GUIs from your local workstation.

5.13 Hardware Maintenance Administration Tasks

> This section gives instructions on how to prepare hardware for maintenance and how to return hardware back into the deployment.

Maintenance activities include firmware updates, for example.

The following infrastructure components are included in this section:

— ENM Management Server

— ENM nodes

— HP c7000 Onboard Administrator

— HP c7000 Virtual Connect

— HP c7000 Brocade switches

— Dell EMC Unity SAN

— EMC SAN VNX

— NAS cluster

Prerequisites

— An installation or upgrade must not be in progress during this procedure.

Result

ENM hardware is made available for maintenance and returned to the deployment following maintenance update.

5.13.1 Node Hardware Update

> This section gives instructions on how to perform a maintenance update of ENM nodes.

Perform this procedure any time a node needs to be temporarily removed from the ENM deployment for maintenance.

For maintenance updates of all nodes, perform updates in the following order:

— All DB nodes.

— All SCP nodes.

— All SVC nodes.

— All EVT nodes.

— All STR nodes.

— All ASR nodes.

— All EBS nodes.

— All EBA nodes.

Prerequisites

— You have `litp-admin` and `root` access to nodes.

Result

All nodes in the deployment are updated to the desired specification.

5.13.1.1 Pre-Update Steps for Node Hardware

1. To remove the Target node from the cluster, complete the following steps.
2. From a terminal window, log on to the target node as the `litp-admin` user, then switch to the `root` user:

   In this instance, db-2.

```
[root@ms ~]# ssh litp-admin@db-2
Password:
[litp-admin@db-2 ~]$ su -
Password:
[root@db-2 ~]#
```

3. From a second terminal, log on to the other DB node to monitor the Target DB node as the `litp-admin` user, then switch to the `root` user.

   In this instance, db-3.

```
[root@ms ~]# ssh litp-admin@db-3
Password:
[litp-admin@db-3 ~]$ su -
Password:
[root@db-3 ~]#
```

4. On the monitoring node, watch the status of the target node by entering the following command:

```
[root@db-3 ~]# watch -n0 hastatus -summary
Every 0.1s: hastatus -summary                                                  →


-- SYSTEM STATE
-- System               State                Frozen

A  db-1                 RUNNING              0
A  db-2                 RUNNING              0
A  db-3                 RUNNING              0
A  db-4                 RUNNING              0
```

5. On the target node, freeze the node by entering the following command:

```
[root@db-2 ~]# haconf -makerw
[root@db-2 ~]# hasys -freeze -persistent -evacuate <node>

Example
[root@db-2 ~]# haconf -makerw
[root@db-2 ~]# hasys -freeze -persistent -evacuate ieatrcxb5256
```

   The monitoring node shows the target node as frozen:

```
Every 0.1s: hastatus -summary                                                  →


-- SYSTEM STATE
-- System               State                Frozen

A  db-1                 RUNNING              0
A  db-2                 RUNNING              1
A  db-3                 RUNNING              0
A  db-4                 RUNNING              0
```

6. Log on to the ENM MS as the `litp-admin` user, then switch to the `root` user. Check that each `ServiceState` on the target node is `OFFLINE`:

```
[root@ms ~]# /opt/ericsson/enminst/bin/vcs.bsh --groups -s <node>


Example
[root@ms ~]# /opt/ericsson/enminst/bin/vcs.bsh --groups -s db-2
```

```
Getting groups from cluster db_cluster on system ieatrcxb5240
  ----------  --------------------------------------------------  ----------- →
-  --------------  -----------  ------------  ----------  ------
     Cluster                                                Group        Syste →
m          HAType  ServiceType  ServiceState  GroupState  Frozen
  ----------  --------------------------------------------------  ----------- →
-  --------------  -----------  ------------  ----------  ------
  db_cluster           Grp_CS_db_cluster_jms_clustered_service  db-2         →
    active-standby          lsb       OFFLINE          OK       -
  db_cluster  Grp_CS_db_cluster_modeldeployment_cluster_service  db-2         →
    active-standby          lsb       OFFLINE          OK       -
  db_cluster       Grp_CS_db_cluster_postgres_clustered_service  db-2         →
    active-standby          lsb       OFFLINE          OK       -
  db_cluster    Grp_CS_db_cluster_sg_neo4jbur_clustered_service  db-2         →
    active-standby          lsb       OFFLINE          OK       -
  db_cluster  Grp_CS_db_cluster_elasticsearch_clustered_service  db-2         →
    active-standby          lsb       OFFLINE          OK       -
  db_cluster         Grp_CS_db_cluster_opendj_clustered_service  db-2         →
          parallel          lsb       OFFLINE     Invalid       -
  db_cluster       Grp_CS_db_cluster_sg_neo4j_clustered_service  db-2         →
    active-standby          lsb       OFFLINE          OK       -
  ----------  --------------------------------------------------  ----------- →
-  --------------  -----------  ------------  ----------  ------
```

Note: Repeat this check until each `ServiceState` is `OFFLINE` before moving to the next step.

7. On the target node, make the target node read-only:

```
[root@db-2 ~]# haconf -dump -makero
```

8. On the target node, stop the VCS service:

```
[root@db-2 ~]# service vcs stop
Confirming that HAD has unregistered with GAB (retry 1)    [  OK  ]
HAD has unregistered with GAB
  PID TTY          TIME CMD
[root@db-2 ~]#
```

9. The monitoring node shows an `EXITED` state on the target node:

```
Every 0.1s: hastatus -summary                                               →
 Thu Oct 17 09:41:42 2019

-- SYSTEM STATE
-- System               State                Frozen

A  db-1                 RUNNING               0
A  db-2                 EXITED                1
A  db-3                 RUNNING               0
A  db-4                 RUNNING               0
```

10. On the target node, issue a shutdown command:

```
[root@db-2 ~]# shutdown -h 0
```

Results

The target node is now removed from the cluster, and is ready for maintenance activities.

Note: The hardware is now available for maintenance update.

5.13.1.2 Post-Update Steps for Node Hardware

1. To add the node back into the cluster, complete the following steps:
2. Once the node hardware update is complete, log on to the target node as the `litp-admin` user and switch to the `root` user.

```
[root@ms ~]# ssh litp-admin@db-2
Password:
[litp-admin@db-2 ~]$ su -
Password:
[root@db-2 ~]#
```

3. Open a second connection towards the monitoring node, if one is not already open.

```
[root@ms ~]# ssh litp-admin@db-1
Password:
[litp-admin@db-1 ~]$ su -
Password:
[root@db-1 ~]#
```

4. On the monitoring node, watch the status of the target node:

```
[root@db-1 ~]# watch -n0 hastatus -summary
```

5. On the target node, unfreeze the node:

```
[root@db-2 ~]# haconf -makerw
[root@db-2 ~]# hasys -unfreeze -persistent <node>
```

   Example

```
[root@db-2 ~]# haconf -makerw
[root@db-2 ~]# hasys -unfreeze -persistent db-2
```

   The monitoring node shows the target node as `RUNNING` and no longer frozen:

```
Every 0.1s: hastatus -summary                    Tue Nov 17 10:54:43 2015

-- SYSTEM STATE
-- System               State                Frozen
A  db-1                 RUNNING              0
A  db-2                 RUNNING              0
```

6. On the target node, write the changes to disk and make the cluster read-only.

```
[root@db-2 ~]# haconf -dump -makero
```

7. On the target node, restart the VCS service.

```
[root@db-2 ~]# service vcs restart
```

The monitoring node shows the target node as `EXITED` and groups as `OFFLINE`, before returning to a `RUNNING` state and `ONLINE` groups:

```
Every 0.1s: hastatus -summary                                    Tue Nov 17
11:14:43 2015

-- SYSTEM STATE
-- System               State                Frozen
A  db-1                 RUNNING              0
A  db-2                 RUNNING              0
```

8. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.

```
[root@ms ~]# /opt/ericsson/enminst/bin/vcs.bsh --groups -s <node>
```

Note: Repeat this check until each `GroupState` reads `OK` before moving to Step 9.

9. Check that each on the target node reads OK:

   When on a two node DB cluster (Medium or Large ENM Systems), check that the service groups are in a balanced state.

   When inserting a node back into the ENM DB cluster, ensure the service groups are balanced correctly. On the ENM MS, run the following command:

```
[root@ms ~]# cd /opt/ericsson/enminst/lib/
[root@ms lib]# python -c "import switch_db_groups; switch_db_groups.switch_d
bcluster_groups()"
```

   Example output:

```
[root@ms lib]# python -c "import switch_db_groups; switch_db_groups.switch_d
bcluster_groups()"
2017-02-27 17:32:33 INFO  switch_dbcluster_groups       : Distributing Activ
e-Standby Service Groups among the systems in DB cluster
2017-02-27 17:32:41 INFO  switch_dbcluster_groups       : SG distribution fi
nished
```

Note: This check must NOT be performed on four node DB clusters (Extra Large ENM systems).

10. On the ENM MS, confirm that each `GroupState` in the cluster reads `OK` by entering the following command:

```
[root@ms ~]# /opt/ericsson/enminst/bin/vcs.bsh --groups
```

11. Ensure Neo4j instance on the maintained node is catching up to the Cluster leader:

Note: Step 11 to Step 14 are only applicable if Neo4j is running in Causal Cluster mode (60K deployment).

There is a possibility that the Neo4j instance can go out of sync with the leader and never catch up.

Complete the following steps to find out the leader in the casual cluster:

a. Log on to the ENM MS as the `litp-admin` user, then switch to the `root` user. Run the following command to know the db details running with the Neo4j service.

```
[root@ms ~ ]# cd /opt/ericsson/enminst/bin/
[root@ms bin]# ./vcs.bsh --group -c db_cluster -g Grp_CS_db_cluster →
_sg_neo4j_clustered_service
Getting groups from cluster Getting groups from cluster db_cluster  →
on system ms
  ----------  ------------------------------------------  ------- →
-----  --------  -----------  ------------  ----------  ------
     Cluster                                          Group        S →
ystem    HAType  ServiceType  ServiceState  GroupState  Frozen
  ----------  ------------------------------------------  ------- →
-----  --------  -----------  ------------  ----------  ------
  db_cluster  Grp_CS_db_cluster_sg_neo4j_clustered_service  db-2     →
       parallel          lsb        ONLINE          OK       -
  db_cluster  Grp_CS_db_cluster_sg_neo4j_clustered_service  db-3     →
       parallel          lsb        ONLINE          OK       -
  db_cluster  Grp_CS_db_cluster_sg_neo4j_clustered_service  db-4     →
       parallel          lsb        ONLINE          OK       -
  ----------  ------------------------------------------  ------- →
-----  --------  -----------  ------------  ----------  ------
```

b. To find the `LEADER` in casual cluster, log on to any one of the db where Neo4j service is running as a `root` user, then run the following command:

   In this instance, `db-2/db-3/db-4`.

```
[ root@ms ~ ]# ssh litp-admin@db-2
litp-admin@db-2's password:


[litp-admin@db-2 /]$ su -
Password:


[root@ieatrcxb3912 /]#  /opt/ericsson/neo4j/util/dps_db_admin.py cl →
uster
+--------------+----------+------+---------+----------------------  →
---------------+-----------------------------------------------------  →
--+----------+--------+
|   Instance   |   Role   | Ping | Version |                  ID     →
               |                    Addresses                        →
  | Database | Groups |
+--------------+----------+------+---------+----------------------  →
---------------+-----------------------------------------------------  →
--+----------+--------+
|              | LEADER   | Yes  |  3.5.9  | 75dcbade-40ae-4fff-84a →
9-02c74a8fe9cf | bolt://10.247.246.15:7687 http://10.247.246.15:747  →
4 | default  |   []   |
|    (db-2)    |          |      |         |                        →
               |            https://10.247.246.15:7473              →
  |          |       |
|--------------|----------|------|---------|----------------------  →
---------------|-----------------------------------------------------  →
--|----------|--------|
|              | FOLLOWER | Yes  |  3.5.9  | b8aec49e-cdab-43af-826 →
7-41f5b11dd761 | bolt://10.247.246.19:7687 http://10.247.246.19:747  →
4 | default  |   []   |
|    (db-3)    |          |      |         |                        →
               |            https://10.247.246.19:7473              →
  |          |       |
|--------------|----------|------|---------|----------------------  →
```

```
---------------|-------------------------------------------------
--|----------|--------|
|              | FOLLOWER | Yes  |  3.5.9  | 2fd3758e-6022-4a9e-947
b-5df7e9679b65 | bolt://10.247.246.16:7687 http://10.247.246.16:747
4 | default  |   []   |
|    (db-4)    |          |      |         |
               |            https://10.247.246.16:7473
  |          |        |
+--------------+----------+------+---------+----------------------
---------------+-------------------------------------------------
--+----------+--------+
```

In this instance, `db-2` is the leader.

12. To verify lagging, run `FollowerLaggingMonitor_ddc.sh` on db nodes:

    Note: First run the script as a `root` user on the node where a current leader is running, then on the node that was turned off for maintenance.

```
[root@db-2 litp-admin]# /opt/ericsson/neo4j/scripts/FollowerLaggingMonitor_d
dc.sh
```

The script records the latest committed transaction on the leader and compares it with the follower's latest committed transaction.

Note: Run the script for at least 30 minutes to make sure that followers are not lagging under the load.

13. The output of the script is logged to `/ericsson/tor/data/lagging_monitor/` for each Neo4j instance.

    Monitor these logs for the next 30 minutes. If the follower is lagging a Leader by more than 5 minutes then contact Ericsson Support to raise a support ticket with the Neo4j support group.

    Example

    Sample output when followers are synced up with the leader, in the log file we see a message like 'No lagging on Follower'.

    In this instance, db-2 is LEADER, and db-3 and db-4 are FOLLOWERS.

```
*** LEADER LOG ***
Mon Oct 21 14:19:29 IST 2019    [Lagging_monitor]       [db-2]  [INFO]  Chec
king IP addresses of different Neo4j cluster members.
Mon Oct 21 14:19:30 IST 2019    [Lagging_monitor]       [db-2]  [INFO]  LEAD
ER Ip is : 10.247.246.17
Mon Oct 21 14:19:31 IST 2019    [Lagging_monitor]       [db-2]  [INFO]  FOLL
OWER Ip is : 10.247.246.10
Mon Oct 21 14:19:31 IST 2019    [Lagging_monitor]       [db-2]  [INFO]  FOLL
OWER Ip is : 10.247.246.16
Mon Oct 21 14:19:31 IST 2019    [Lagging_monitor]       [db-2]  [INFO]  Runn
ing on LEADER...
Mon Oct 21 14:19:31 IST 2019    [Lagging_monitor]       [db-2]  [INFO]  Star
t to monitor lagging of committed transactions between Leader : 10.247.246.1
7 and Followers: 10.247.246.10
10.247.246.16
Mon Oct 21 14:19:31 IST 2019    [Lagging_monitor]       [db-2]  [INFO]  The
LastCommittedTxId on Leader is : 1588218682 @ 2019-10-21 14:19:31,979
Mon Oct 21 14:19:31 IST 2019    [Lagging_monitor]       [db-2]  [INFO]  Resu
me check after interval 2 sec.
```

```
*** FOLLOWER LOG ***

Mon Oct 21 13:58:20 IST 2019    [Lagging_monitor]       [db-3]  [INFO]  Chec →
king IP addresses of different Neo4j cluster members.
Mon Oct 21 13:58:21 IST 2019    [Lagging_monitor]       [db-3]  [INFO]  LEAD →
ER Ip is : 10.247.246.17
Mon Oct 21 13:58:22 IST 2019    [Lagging_monitor]       [db-3]  [INFO]  FOLL →
OWER Ip is : 10.247.246.10
Mon Oct 21 13:58:22 IST 2019    [Lagging_monitor]       [db-3]  [INFO]  FOLL →
OWER Ip is : 10.247.246.16
Mon Oct 21 13:58:22 IST 2019    [Lagging_monitor]       [db-3]  [INFO]  Runn →
ing on FOLLOWER...
Mon Oct 21 13:58:22 IST 2019    [Lagging_monitor]       [db-3]  [INFO]  Star →
t to monitor lagging of committed transactions between Leader : 10.247.246.1 →
7 and Followers: 10.247.246.10
10.247.246.16
Mon Oct 21 13:58:22 IST 2019    [Lagging_monitor]       [db-3]  [INFO]  Chec →
king for any lagging of commit transaction ID: 1511816941 on Follower: 10.24 →
7.246.10
Mon Oct 21 13:58:22 IST 2019    [Lagging_monitor]       [db-3]  [INFO]  No l →
agging on Follower: 10.247.246.10 for transaction id: 1511816941. The LastCo →
mmittedTxId on this follower : 1587792598
```

Example

Sample output when the follower is lagging, in the log file we see a message like 'Lagging on Follower'.

```
*** FOLLOWER LOG ***

Mon Oct 21 14:23:07 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  Chec →
king IP addresses of different Neo4j cluster members.
Mon Oct 21 14:23:08 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  LEAD →
ER Ip is : 10.247.246.17
Mon Oct 21 14:23:10 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  FOLL →
OWER Ip is : 10.247.246.10
Mon Oct 21 14:23:10 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  FOLL →
OWER Ip is : 10.247.246.16
Mon Oct 21 14:23:10 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  Runn →
ing on FOLLOWER...
Mon Oct 21 14:23:10 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  Star →
t to monitor lagging of committed transactions between Leader : 10.247.246.1 →
7 and Followers: 10.247.246.10
10.247.246.16
Mon Oct 21 14:23:10 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  Chec →
king for any lagging of commit transaction ID: 1588277143 on Follower: 10.24 →
7.246.16
Mon Oct 21 14:23:10 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  Foun →
d lagging on Follower: 10.247.246.16. The LastCommittedTxId value on the fol →
lower is : 1588274760 @ 2019-10-21 14:23:10,272
Mon Oct 21 14:23:10 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  Lagg →
ing on Follower: 10.247.246.16 so far (in millsec.) : 1796
Mon Oct 21 14:23:10 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  Foun →
d lagging on Follower: 10.247.246.16. The LastCommittedTxId value on the fol →
lower is : 1588274760 @ 2019-10-21 14:23:10,314
Mon Oct 21 14:23:10 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  Lagg →
ing on Follower: 10.247.246.16 so far (in millsec.) : 1838
Mon Oct 21 14:23:10 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  Foun →
d lagging on Follower: 10.247.246.16. The LastCommittedTxId value on the fol →
lower is : 1588274760 @ 2019-10-21 14:23:10,338
Mon Oct 21 14:23:10 IST 2019    [Lagging_monitor]       [db-4]  [INFO]  Lagg →
ing on Follower: 10.247.246.16 so far (in millsec.) : 1862
```

14. After lagging is verified, and none of the followers are behind:

    — Stop script execution on all the nodes.

    — On both leader and follower nodes, remove all files associated with the script as follows:

```
[root@db-3 ~ ]# cd /ericsson/tor/data/lagging_monitor
[root@db-3 lagging_monitor]# rm -rf ./*
```

5.13.2 ENM Management Server Update

This section gives instructions to system administrators and hardware installation engineers on how to prepare the ENM Management Server (MS) for maintenance. The shutdown and update procedures are performed whenever hardware maintenance tasks need to be done on the ENM MS. Updating firmware is an example of such a task.

While the ENM MS is shutdown, the following services and activities are unavailable:

— Puppet Server service.

— ENM System Monitoring (ESM) service.

— Sentinel Deployment and License Management service.

— Diagnostic Data Collection (DDC) service.

— Failing Active-Passive service groups may not successfully switch over, as the image data may need to be read from the MS repository. This is true only if this is the first time that a failover has occurred.

Prerequisites

— The ENM MS is available for updating.

— `root` access to ENM MS.

— System impacts of the ENM MS shutdown have been read and understood.

Result

The ENM MS is available for maintenance and returned to the deployment following maintenance update.

5.13.2.1 Pre-Update Steps for ENM Management Server

Instructions to system administrators and hardware installation engineers on how to prepare the ENM Management Server (MS) for maintenance. The shutdown and update procedures are performed whenever hardware maintenance tasks need to be done on the ENM MS. Updating firmware is an example of such a task.

Note: While the ENM MS is shutdown, the following services and activities are unavailable:

- Puppet Server service.
- ENM System Monitoring (ESM) service.
- Sentinel Deployment and License Management service.
- Diagnostic Data Collection (DDC) service.
- Failing Active-Passive service groups may not successfully switch over, as the image data may need to be read from the MS repository. This is true only if this is the first time that a failover has occurred.

Prerequisites

- The ENM MS is available for updating.
- `root` access to ENM MS.
- System impacts of the ENM MS shutdown have been read and understood.

Expected Result

The ENM MS is available for maintenance and returned to the deployment following maintenance update.

Pre-Update Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. Ensure that no LITP plans are running.

   ```
   [root@ms ~]# litp show_plan | grep -E "^Tasks|^Plan Status"
   Tasks: 1972 | Initial: 0 | Running: 0 | Success: 1972 |
   Failed: 0 | Stopped: 0 Plan Status: Successful [root@ms ~]#
   ```

   Confirm that the `Running` parameter returns `0` running tasks. If there are any plans or tasks running, wait until they have completed before proceeding.
3. Execute a shutdown.

   ```
   [root@ms ~]# shutdown -h 0
   ```

Maintenance Update

Note: The hardware is now available for maintenance update.

5.13.2.2 Post-Update Steps for ENM Management Server

1. After the hardware is updated and the system has rebooted, check that all the nodes can be contacted:

```
[root@ms-1 ~]# mco ping
enmscp2                                  time=25.90 ms
enmdb1                                   time=26.64 ms
enmscp1                                  time=27.52 ms
enmsvc1                                  time=28.19 ms
enmdb2                                   time=28.83 ms
enmsvc2                                  time=29.47 ms
enmevt1                                  time=28.83 ms
enmevt2                                  time=29.47 ms
enmstr1                                  time=30.48 ms
enmstr2                                  time=29.01 ms
enmesa1                                  time=29.76 ms
enmesa2                                  time=29.26 ms
ms-1                                     time=31.60 ms

---- ping statistics ----
9 replies max: 31.60 min: 25.90 avg: 28.31
[root@ms-1 ~]#
```

   If there is no response from a node, log on to the node as the litp-admin user, switch to the root user, and restart the `mcollective` service.

```
[root@ms ~]# ssh litp-admin@enmdb1
Password:
[litp-admin@enmdb1 litp-admin ~]$ su -
Password:
[root@enmdb1 ~]# service mcollective restart
Shutting down mcollective:                                 [  OK  ]
Starting mcollective:                                      [  OK  ]
[root@enmdb1 ~]#
```

   After this has completed successfully on all affected nodes, run `mco ping` again on the MS to verify the connection to each node on the ENM deployment.

5.13.3 Check Validity of SAN Security Certificates

Certain activities on the ENM Management Server (MS), such as a hardware change, can cause existing SAN security certificates to become invalid. This can cause a LITP plan failure if the plan involves changes to the Storage Area Network (SAN) storage configuration.

This section describes the procedure to check the certificates and remove them in the case they become invalid.

Steps

For Unity, do the following:

— Check Validity of Uemcli Security Certificates on page 42

For VNX, do the following:

— Check Validity of Naviseccli Security Certificates on page 43

5.13.3.1 Check Validity of Uemcli Security Certificates

Certain activities on the ENM Management Server (MS), such as a hardware change, can cause existing uemcli security certificates to become invalid. This can cause a LITP plan failure if the plan involves changes to the Storage Area Network (SAN) storage configuration.

This section describes the procedure to check the certificates and remove them in the case they become invalid.

Prerequisites

— `Uemcli` rpm is installed on the MS.

Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. List the certificates as follows:

   ```
   [root@ms]# /usr/bin/uemcli -certList
   ```

   If output similar to the example below is observed, the certificates are invalid and need to be removed.

   ```
   Operation failed. Error code: 0x1000002
   The system encountered an unexpected error Record the error code and go to t →
   he EMC Online Support website for all your support options.
   ```

3. Remove the certificates:

   ```
   [root@ms]# /usr/bin/uemcli -certClear
   ```

4. Verify that the certificates were removed:

   ```
   [root@ms]# /usr/bin/uemcli -certList
   ```

   The above command produces no output if the certificates were successfully removed.

Results

Unity security certificates on the MS are checked and removed, if found to be invalid.

5.13.3.2 Check Validity of Naviseccli Security Certificates

Certain activities on the ENM Management Server (MS), such as a hardware change, can cause existing Naviseccli security certificates to become invalid. This can cause a LITP plan failure if the plan involves changes to the Storage Area Network (SAN) storage configuration.

This section describes the procedure to check the certificates and remove them in the case they become invalid.

Note: The certificates are stored under the `/` and `/root` directories. Run the steps of this procedure for each directory.

Prerequisites

— `NaviCLI` rpm is installed on the MS.

Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. Set the HOME environmental variable for `/` directory:

   ```
   [root@ms]# export HOME=/
   ```

   Note: When repeating this procedure to check the certificates for /root directory, set the HOME variable as follows:

   ```
   [root@ms]# export HOME=/root
   ```

3. List the certificates as follows:

   ```
   [root@ms]# /opt/Navisphere/bin/naviseccli security -certificate -list
   ```

   If output similar to the example below is observed, the certificates are invalid and need to be removed.

   ```
   Error occurred while trying to connect: '10.0.2.5'.
   Message : A library or configuration file for NaviSECCli is missing or corru →
   pt. Please use command "security -certificate -cleanup" to fix it. If you st →
   ill have the same issue, please re-install NaviSECCli.
   ```

4. Remove the certificates:

   ```
   [root@ms]# /opt/Navisphere/bin/naviseccli security -certificate -cleanup
   ```

5. Verify that the certificates were removed:

   ```
   [root@ms]# /opt/Navisphere/bin/naviseccli security -certificate -list
   ```

The above command produces no output if the certificates were successfully removed.

Results

Naviseccli security certificates on the MS are checked and removed, if found to be invalid.

5.13.4 OA, VC and Brocade Hardware Update

> This section gives instruction on how to make the Onboard Administrator (OA) modules, Virtual Connect (VC) modules and Brocade switches available for maintenance.

Prerequisites

— Components are available for updating.

Result

Hardware components are made available for maintenance and returned to the deployment following maintenance update.

Pre-Update Steps

Not applicable to this maintenance update.

Hardware Update

Note: The hardware is now available for maintenance update.

Post-Update Steps

Not applicable to this maintenance update.

5.13.5 SAN Hardware Update

> This section gives instruction on how to make the SAN hardware available for maintenance and return it to the deployment following maintenance update.

For Unity, do the following:

— Pre-Update Steps for Dell EMC Unity Hardware on page 45

— Post-Update for Dell EMC Unity Hardware Update on page 46

For VNX, do the following:

— Pre-Update Steps for EMC VNX Hardware on page 46

— Post-Update for EMC VNX Hardware Update on page 46

Result

SAN hardware is made available for maintenance and returned to the deployment following maintenance update.

5.13.5.1 Pre-Update Steps for Dell EMC Unity Hardware

1. Perform a health check of the entire system. Before upgrading system software, a system health check must be performed.

    a. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user and enter the following command:

    ```
    [root@ms ~]# /usr/bin/uemcli -d <sp_ip> /sys/general healthcheck
    ```

    Example

    ```
    [root@ms ~]# /usr/bin/uemcli -d 10.45.22.54 /sys/general healthchec
    k
    Storage system address:10.45.22.544
    Storage system port: 443
    HTTPS connection

    Operation completed successfully.
    [root@ms ~]#
    ```

    Note: In UEMCLI The results of the health check may show errors and warnings, but a message of operation completed successfully displays in the output. This is only an indication that the health check action was performed, not that it was successfully completed without errors and warnings. Attempt to resolve all errors and rerun the health check. If errors occur, a system software upgrade is not allowed. If warnings occur, they can be bypassed during the upgrade procedure

After This Task

Hardware Update

Note: The hardware is now available for maintenance update.

In cases when SAN switches are replaced or rebooted no loss of service is expected in ENM. However, you may encounter that the UI becomes non-responsive for about 30 seconds and observe monitor timeouts on various VMs. Disregard the monitor timeouts.

5.13.5.2 Post-Update for Dell EMC Unity Hardware Update

Not applicable to this maintenance update.

5.13.5.3 Pre-Update Steps for EMC VNX Hardware

1. Verify that the load on the VNX does not exceed 50%.

    a. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user and enter the following command:

    ```
    [root@ms ~]# naviseccli -h <SPA IP address> getcontrol | grep "Prct
     Busy"
    ```

    Example

    ```
    [root@ms ~]# naviseccli -h 10.32.229.46 getcontrol | grep "Prct Bus
    y"
    Prct Busy:        2.59
    [root@ms ~]#
    ```

    b. Repeat step 1a on SPB.

After This Task

Hardware Update

Note: The hardware is now available for maintenance update.

In cases when SAN switches are replaced or rebooted no loss of service is expected in ENM. However, you may encounter that the UI becomes nonresponsive for about 30 seconds and observe monitor timeouts on various VMs. Disregard the monitor timeouts.

5.13.5.4 Post-Update for EMC VNX Hardware Update

Not applicable to this maintenance update.

5.13.6 SAN Disk Replacement

In the event of a disk failure as notified by ESM, this section describes the procedure for replacing faulted disk.

For Unity, do the following:

— Dell EMC Unity Disk Replacement on page 47

For VNX, do the following:

— EMC VNX Disk Replacement on page 47

5.13.6.1 Dell EMC Unity Disk Replacement

In the event of a disk failure, this section describes the procedure for replacing the faulted disk.

Steps

1. Contact DELL EMC Support to replace the faulted disk.

   In Dell EMC Unity All-Flash models 300 and 450F, running OE version 4.2.x or later, all new pools created in the Unisphere GUI are dynamic pools, and new pools created in the Unisphere CLI and REST API are dynamic pools by default. Dynamic pools implement advanced RAID technology. In dynamic pools, a RAID group is spread across drive extents in multiple drives. The required spare space is also spread across drive extents in multiple drives. When a drive fails, the extents on the failed drive are rebuilt to spare space extents within the pool.

   Note: It is advisable to replace failed disks as soon as possible. Rebuild times are usually much faster than with traditional pools. Since spare capacity for a dynamic pool is spread across multiple drives rather than concentrated in on a single hot spare drive, more drives contribute to the rebuilding process when a drive fails.

Results

The replacement disk is inserted into the SAN DPE.

5.13.6.2 EMC VNX Disk Replacement

In the event of a disk failure as notified by ESM, this section describes the procedure for replacing faulted EMC disk.

Steps

1. Contact EMC Support to replace the faulted disk.

   For models VNX5200 and VNX5400 EMC Hot Spare technology allows for any unbound disk to be considered for sparing. This used Spare now becomes a permanent member of the Storage Pool, no reconfiguration is required. When the failed drive gets replaced it becomes a Spare for eligible drives within the entire VNX Array.

   For models VNX5100, VNX5300 and VNX5500 the Hot Spare is dedicated and the replacement disk needs to be rebuilt from the Hot Spare.

Note: It is advisable to replace failed disks as soon as possible to ensure that the deployment adheres to the recommended Hot Spare Policy.

Results

The replacement disk is inserted into the SAN DAE.

5.13.7 Replace HPE Blade

If there is a faulted HPE Blade in use in an ENM cluster, then replace it using the following steps.

Prerequisites

— The replacement blade has the same characteristics as the faulted blade, including HBA and NIC cards.

— Node name and IP addresses of the faulted node are known.

— The hostname of the faulted HPE Blade is to be reused for the replacement blade.

— There is no failed LITP plan in place.

— You have Administrator access to the Virtual Connect (VC), Onboard Administrator (OA) and Unisphere Admin GUI.

— You have Administrator access to the ENM MS and MNs.

— You have Administrator access to the Brocade SAN switches.

— You have the password for accessing the interactive GRUB menu.

— You have the password for the root user on the faulted blade.

— You have access to the iLO console of the replacement blade.

Blade Replacement Flow

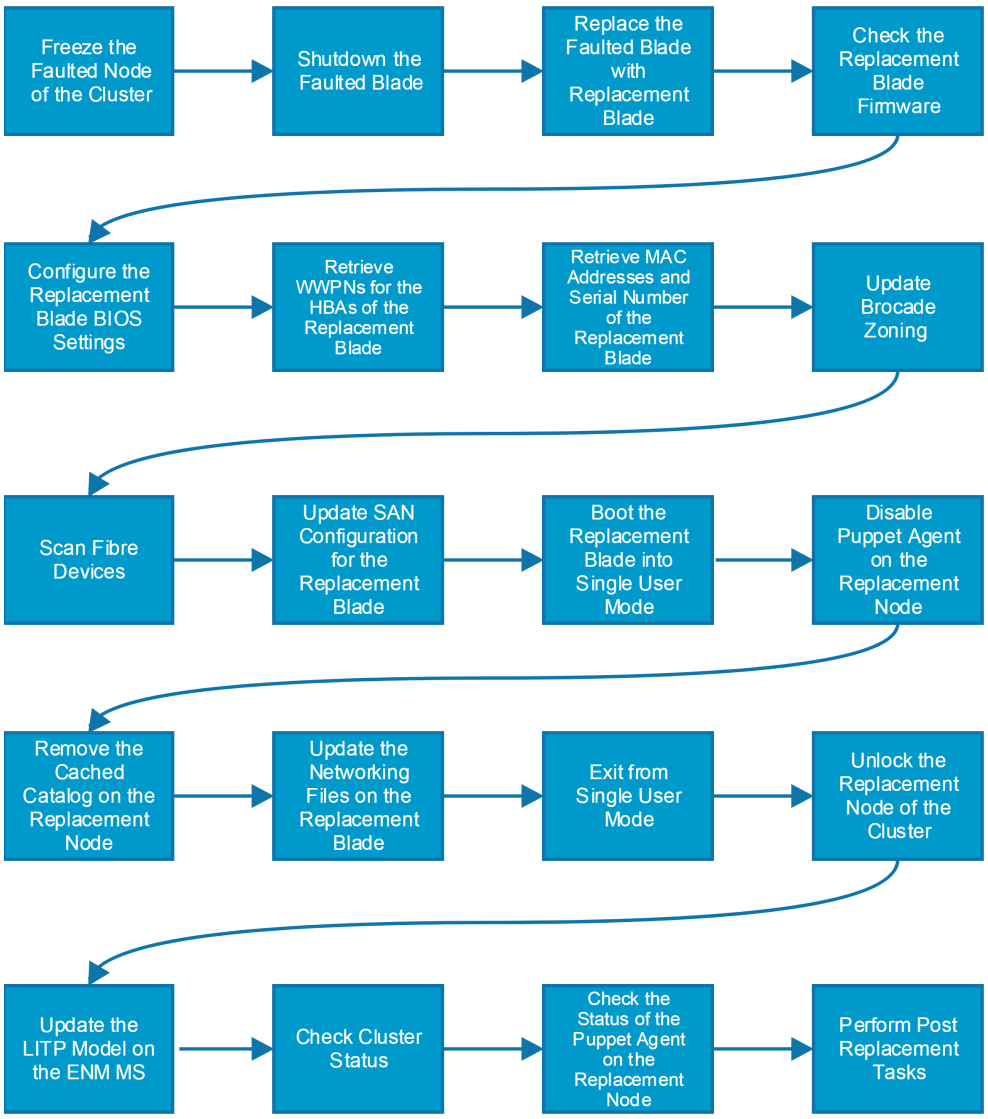


Figure 1 Blade Replacement Flow

Steps

1. Freeze the Faulted Node of the Cluster on page 50
2. Shut Down the Faulted Blade on page 52
3. Replace the Faulted Blade with Replacement Blade on page 52
4. Check the Replacement Blade Firmware on page 53

5. Configure the Replacement Blade BIOS Settings on page 53
6. Retrieve WWPNs for the HBAs of the Replacement Blade on page 53
7. Retrieve MAC Addresses and Serial Number of the Replacement Blade on page 54
8. Update Brocade Zoning on page 56
9. Scan Fibre Devices on page 56
10. Update SAN Configuration for the Replacement Blade on page 58
11. Boot the Replacement Blade into Single User Mode on page 66
12. Disable Puppet Agent on the Replacement Node on page 67
13. Remove the Cached Catalog on the Replacement Node on page 67
14. Update the Networking Files on the Replacement Blade on page 68
15. Exit from Single User Mode on page 70
16. Unlock the Replacement Node of the Cluster on page 71
17. Update the LITP Model on the ENM MS on page 72
18. Check Cluster Status on page 73
19. Check the Status of the Puppet Agent on the Replacement Node on page 74
20. Perform Post Replacement Tasks on page 74

Note: For rollbacks, if it is decided to return the cluster to its original state, then use this blade replacement procedure to re-insert the original faulted blade. Skip any unnecessary steps. Before starting the rollback, ensure that the Serial Number, MAC addresses and WWPNs of the original faulted blade are available.

Results

The faulted blade is successfully replaced with a new blade and the peer server is successfully brought back into the ENM cluster with services restored.

5.13.7.1 Freeze the Faulted Node of the Cluster

It is recommended to cleanly fail over services from the faulted node to another node in its cluster. If services are failed over already, then skip this task and proceed to Shut Down the Faulted Blade.

Steps

1. Log on as the `litp-admin` user from the ENM MS to another node in the same cluster of the node to freeze.
2. Switch to the `root` user:

```
[litp-admin@node-2 ~]$ su -
```

3. Freeze the node, where <node_name> represents the name of the node:

```
[root@node-2 ~]# haconf -makerw
[root@node-2 ~]# hasys -freeze -persistent -evacuate <node_name>
[root@node-2 ~]# haconf -dump -makero
```

Example

```
[root@node-2 ~]# haconf -makerw
[root@node-2 ~]# hasys -freeze -persistent -evacuate node-1
[root@node-2 ~]# haconf -dump -makero
```

This example shows the `node-1` node frozen by commands executed on the `node-2`

4. Confirm that the node is frozen:

```
[root@node-2 ~]# hastatus -sum
```

The following example shows that `node-1` is frozen.

Example

```
-- SYSTEM STATE
-- System         State                Frozen

A  node-1         FAULTED              1
A  node-2         RUNNING              0

-- GROUP STATE
-- Group           System               Probed     AutoDisabled    State      →

B  Grp_CS_svc_cluster_access_control node-1         Y          N               →
   OFFLINE
B  Grp_CS_svc_cluster_access_control node-2         Y          N               →
   ONLINE
B  Grp_CS_svc_cluster_apserv node-1         Y          N               OFFLI →
NE
B  Grp_CS_svc_cluster_apserv node-2         Y          N               ONLIN →
E
B  Grp_CS_svc_cluster_bnsiserv node-1         Y          N               OFF →
LINE
B  Grp_CS_svc_cluster_bnsiserv node-2         Y          N               ONL →
INE
.....
B  Grp_CS_svc_cluster_haproxy_int node-1         Y          N               →
OFFLINE
B  Grp_CS_svc_cluster_haproxy_int node-2         Y          N               →
ONLINE
.....
```

In this example, the value 1 in the `Frozen` column indicates that the faulted `node-1` node is frozen. Any service that was running on `node-1` is either `OFFLINE` or has been switched to `ONLINE` on `node-2`.

Note: If there are no issues with failing over services, then continue with the next step in the procedure

.

Results

Sevices from the faulted node are failed over to another node in the cluster

5.13.7.2 Shut Down the Faulted Blade

This section describes how to shut down the faulted blade.

Note: If possible, check the firmware levels on the faulted blade before shutting it down.

Steps

1. Log on as the `root` user to the iLO of the faulted blade through the ENM MS.
2. Start the Virtual Serial Port (vsp) service:

```
</>hpiLO-> vsp
```

3. Power down the faulted node:

```
[root@node-1 ~]# shutdown -h 0
```

4. If the vsp service is unresponsive in step 2, then shut down the faulted blade from the iLO:

```
</>hpiLO-> power off hard
```

5. Check the power status of the faulted blade.

```
</>hpiLO-> power
```

Results

The faulted blade is shut down.

5.13.7.3 Replace the Faulted Blade with Replacement Blade

This section describes the physical replacement of the hardware.

Steps

1. When the faulted blade is powered down, contact HPE Support to remove the faulted blade from the enclosure and insert the replacement blade into the same bay.

   Note: For hardware commissioning and backup and restore to work with the replacement blade, you must insert it into the same bay as the faulted blade.

Results

The replacement blade is inserted into the enclosure.

5.13.7.4 Check the Replacement Blade Firmware

Ensure that the blade firmware and NIC firmware are at the required levels.

Steps

Check that the blade and NIC firmware are at the levels specified by the FLARE and Firmware Handling guide for HP/EMC.

Results

The blade firmware and NIC firmware are at the required levels.

5.13.7.5 Configure the Replacement Blade BIOS Settings

This task describes how to configure the replacement blade BIOS according to ENM requirements.

Steps

Follow the procedure in the *BIOS Configuration Procedure* chapter of the ENM Installation Instruction.

Results

Replacement blade BIOS settings are configured.

5.13.7.6 Retrieve WWPNs for the HBAs of the Replacement Blade

When the Ericsson recommended interconnect bay layout is followed, the required WWPNs are those assigned to HBA 1 Port 1 and HBA 2 Port 1 of the replacement blade.

Steps

1. Log on as the `root` user to the `Onboard Administrator` using SSH from the ENM MS.

2. Retrieve the WWPN information where `<bay number>` represents the number of the bay where the replacement blade is inserted:

```
oa1> SHOW SERVER PORT MAP <bay number>
```

   Example output:

```
oa1> SHOW SERVER PORT MAP 1
                Mezz
Mezz   Mezz  Device  Port      Interconnect Interconnect
Slot  Device  Port  Status         Bay        Bay Port       Device ID
----  ------ ------ ---------- ------------ ------------ ----------------
------------------------------ Blade 001 ------------------------------
    1 HP QMH2672 16Gb FC HBA for BladeSystem c-Class
           Port 1 OK            Bay 3        Port 1     50:01:43:80:16:7d:b →
2:18
           Port 2 No Connect    Bay 4        Port 1     50:01:43:80:16:7d:b →
2:1a
    2 HP QMH2672 16Gb FC HBA for BladeSystem c-Class
           Port 1 OK            Bay 5        Port 1     50:01:43:80:16:7d:b →
2:38
           Port 2 No Connect    Bay 6        Port 1     50:01:43:80:16:7d:b →
2:3a
 FLB1 HP FlexFabric 10Gb 2-port 536FLB Adapter
Ethernet FlexNIC LOM1:1-a OK     Bay 1        Port 1     A5:C2:17:3F:AC:E0
Ethernet FlexNIC LOM1:1-b OK     Bay 1        Port 1     A5:C2:17:3F:AC:E1
Ethernet FlexNIC LOM1:1-c OK     Bay 1        Port 1     A5:C2:17:3F:AC:E2
Ethernet FlexNIC LOM1:1-d OK     Bay 1        Port 1     A5:C2:17:3F:AC:E3
Ethernet FlexNIC LOM1:2-a OK     Bay 2        Port 1     A5:C2:17:3F:AC:E8
Ethernet FlexNIC (NIC 3) LOM1:2-b OK Bay 2    Port 1     A5:C2:17:3F:AC:E9
Ethernet FlexNIC LOM1:2-c OK     Bay 2        Port 1     A5:C2:17:3F:AC:EA
Ethernet FlexNIC LOM1:2-d OK     Bay 2        Port 1     A5:C2:17:3F:AC:EB
```

   From the previous example output, the required WWPNs are as follows:

```
HBA1 Port1 WWPN = 50:01:43:80:16:7d:b2:18
HBA2 Port1 WWPN = 50:01:43:80:16:7d:b2:38
```

3. Record the values of the WWPNs because you will require the values at a later stage.

Results

Recorded values of the WWPNs for the HBAs of the Replacement Blade

5.13.7.7 Retrieve MAC Addresses and Serial Number of the Replacement Blade

This describes how to retrieve the MAC addresses and serial number of the replacement blade from the Virtual Connect (VC) module.

Steps

1. Log on as the `root` user to the VC using SSH from the ENM MS.

2. Retrieve the name of the Network Profile that is automatically applied to the replacement blade:

```
vc1> show server
```

Example output:

```
==============================================================================
ID      Enclosure  Bay  Description      Status  Power  Profile
==============================================================================
enc0:1  enc1       1    ProLiant         OK      Off    ENM_SE_Bay_1_ie
                        BL460c                          atrcxb5035
------------------------------------------------------------------------------
enc0:2  enc1       2    ProLiant         OK      On     ENM_SE_Bay_2_ie
                        BL460c                             atrcxb5039
------------------------------------------------------------------------------
enc0:3  enc1       3    ProLiant         OK      On     ENM_SE_Bay_3_ie
                        BL460c                             atrcxb5055

------------------------------------------------------------------------------
enc0:5  enc1       5    ProLiant         OK      On     ENM_SE_Bay_5_ie
                        BL460c                             atrcxb5245
------------------------------------------------------------------------------
```

The previous example shows the output for each populated bay. Retrieve the Network Profile name using the number of the bay where the replacement blade is inserted.

3. Retrieve the MAC addresses and serial number where `<profile_name_for_replacement_blade>` is the network profile name retrieved in step 2:

```
-> show profile <profile_name_for_replacement_blade>
```

Example output:

```
->show profile ENM_SE_Bay_3_atrcxb5055
Name                 : ENM_SE_Bay_3_ieatrcxb5055
Device Bay           : enc0:1
Server               : ProLiant BL460c
Status               : OK
Serial Number        : CZ351S3T2P
UUID                 : 33363737-3032-5A43-3335-3238334D3050
NAG                  : Default
Hide Unused FlexNICs : false
UEFI Boot Mode       : Auto
SR-IOV Mode          : Advanced
Ethernet Network Connections
==============================================================================
Port  Network     Status  PXE/IP Boot   MAC Address        Allocated
      Name                Order                            Speed
                                                           (min-max)
==============================================================================
1     Multiple    OK      Enabled/Auto  A5-C2-17-3F-AC-E0  9.9Gb-10Gb
      Network
------------------------------------------------------------------------------
2     Multiple    OK      Disabled/Aut  A5-C2-17-3F-AC-E8  9.9Gb-10Gb
      Network             o
------------------------------------------------------------------------------
3     ENM350_HB1  OK      Disabled/Aut  A5-C2-17-3F-AC-E1  100Mb-10Gb
                          o
------------------------------------------------------------------------------
4     ENM350_HB2  OK      Disabled/Aut  A5-C2-17-3F-AC-E9  100Mb-10Gb
```

```
                                o
--------------------------------------------------------------------------
```

4. Record each of the four MAC addresses and port numbers in the following format for later use. The port numbers map to the interface names as shown in the table.

Port Number	Interface Name	MAC Address (Example)
1	eth0	A5:C2:17:3F:AC:E0
2	eth1	A5:C2:17:3F:AC:E8
3	eth2	A5:C2:17:3F:AC:E1
4	eth3	A5:C2:17:3F:AC:E9

Results

Recorded MAC addresses and serial number of the replacement blade.

5.13.7.8 Update Brocade Zoning

This task describes how to update the Brocade zoning configuration.

Steps

1. Update the Brocade switches zoning configuration to ensure the replacement blades WWPNs have the required access to the San Storage.

   Contact the system administrator of your fabric network to perform the required updates on the Brocade SAN switches.

Results

Brocade switches zoning configuration is updated

5.13.7.9 Scan Fibre Devices

Scan for Fibre devices to ensure that the HBA Initiators are registered on the SAN.

5.13.7.9.1 Gen10 Blades

1. Log on to the iLO of the blade as an administrator user and launch the Remote Console.
2. Boot the blade and press **F9** when prompted to enter the **System Utilities** menu.

3. Select **System Configuration**.

   Note: To identify each of the two host adapters connected to the SAN:

   The first port of the first FC HBA card of the blade maps to the SAN switch in interconnect bay three.

   The first port of the second FC HBA card of the blade maps to the SAN switch in interconnect bay five.

4. Select the first port of the first FC HBA card and select **Scan Fibre Devices**.
5. Select **Select Host Adapter**.
6. Select the first port of the second FC HBA card and select **Scan Fibre Devices**.
7. Reboot the server by pressing **Esc** and then **Enter**.

5.13.7.9.2 Gen9 and Gen8 Blades

1. Log on to the iLO of the blade as an administrator user and launch the Remote Console.
2. Boot the blade and press **Ctrl-Q** when prompted to enter **Fast!UTIL**.

   A menu similar to Figure: QLogic HBA Selection is displayed on-screen.

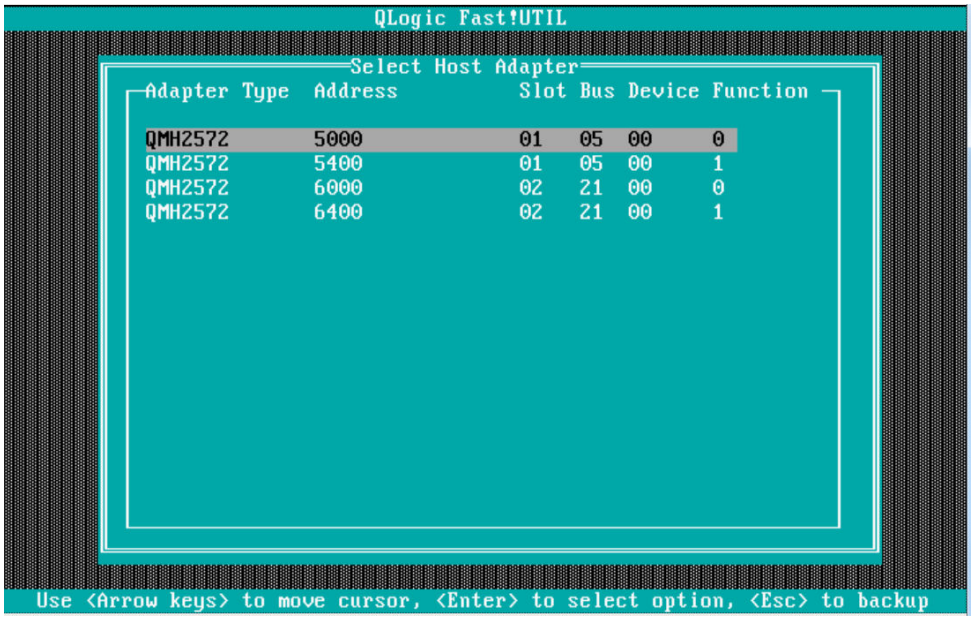


Figure 2 QLogic HBA Selection

Note: To identify each of the two host adapters connected to the SAN:

- The first port of the first fibre HBA card of the blade maps to the SAN switch in interconnect bay three.
- The first port of the second fibre HBA card maps to the SAN switch in interconnect bay five.

3. Select the first port and select Scan Fibre Devices.

   Repeat for the first port for each HBA connected to the SAN. To select a subsequent HBA, select **Select Host Adapter**, then select the appropriate HBA from the menu.

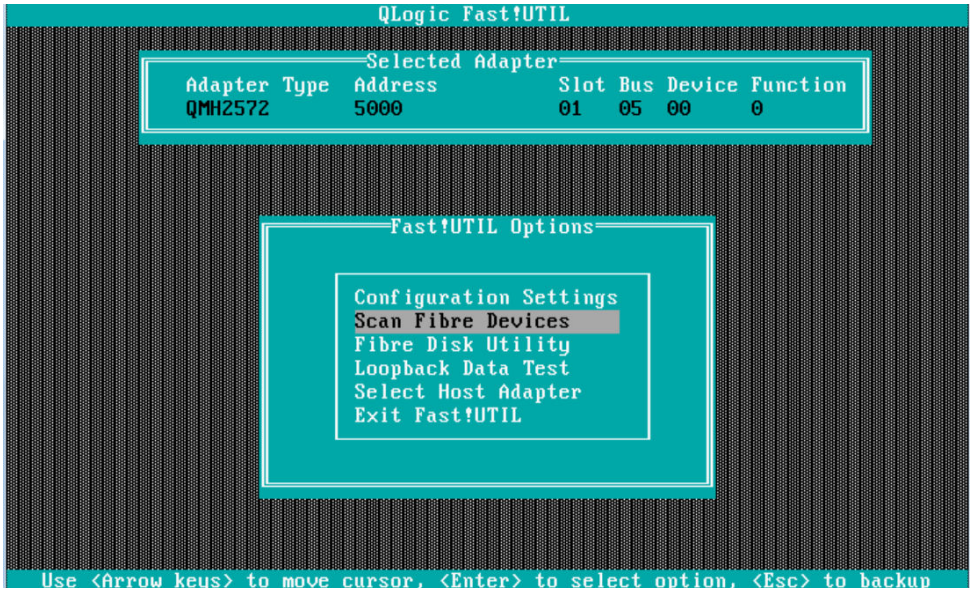


Figure 3 Scan Fibre Devices

4. Reboot the server by pressing **Esc** and then **Enter**.

Results

Scan of Fibre Devices performed and HBA Initiators are visible to the Brocade SAN Switch or storage array.

5.13.7.10 Update SAN Configuration for the Replacement Blade

For Unity, do the following:

- Update Dell EMC Unity SAN Configuration for the Replacement Blade on page 59

For VNX, do the following:

- Update VNX SAN Configuration for the Replacement Blade on page 61

5.13.7.10.1 Update Dell EMC Unity SAN Configuration for the Replacement Blade

> This task describes how to update the SAN configuration to enable the replacement blade to inherit the LUNs of the faulted blade.

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. Use the following command to list all the hosts information where `<sp_ip>` is the IP address of Unity array.

```
[root@ms ~]# /usr/bin/uemcli -d <sp_ip> /remote/host show -detail
```

Example output:

```
...
...

8:    ID              = Host_40
      Name            = SANENM1-enm-svc_cluster-svc-1
      Description     = enmsvc1
      Tenant          =
      Type            = host
      Address         =
      Netmask         =
      OS type         =
      Ignored address =
      Management type = Manual
      Accessible LUNs = sv_4769,sv_4768,sv_4770
      Host LUN IDs    = 0,1,2
      Health state    = Degraded/Warning (10)
      Health details  = "The host does not have any initiators logged into t →
he storage system. Register one or more initiators on the host to the storag →
e system.

...
```

In the previous example output, search for the hostname of the blade that is being replaced, retrieve the ID of the host for the faulty blade. The health state of the host will be Degraded/Warning as the blade is powered off. The host for the faulted blade in this example output has Description set to enmsvc1

3. Get the initiator ID for the WWN (UID) of the host HBAs by running the following command:

```
[root@ms ~]# /usr/bin/uemcli -d <sp_ip> /remote/initiator -unregistered show →
 -filter "ID","UID"
```

Example output:

```
...
...

9:    ID  = HostInitiator_337
      UID = 50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18

10:   ID  = HostInitiator_338
      UID = 50:01:43:80:24:D1:B9:ED:50:01:43:80:16:7D:B2:38
```

```
...
```

The WWPNs are the last 8 bytes of the UID in the previous example output. Match these with the HBA port WWPNs that were collected earlier in the Replacement Blade procedure. Record the IDs of the initiators from the replacement blade.

4. Register the new initiators id's gathered in step 3 with the host identified in step 2, the commands are as follows to register each of the unregistered initiators that were identified.

```
[root@ms]# /usr/bin/uemcli -d <sp_ip> /remote/initiator -id HostInitiator_337 set -host Host_40
```

```
[root@ms]# /usr/bin/uemcli -d <sp_ip> /remote/initiator -id HostInitiator_338 set -host Host_40
```

5. Verify that the initiators have been registered correctly on the host as follows:

```
[root@ms]# /usr/bin/uemcli -d <sp_ip> /remote/initiator -host Host_40 show -
filter "ID,Host,UID,Ignored,Health Details"
```

```


1:    ID                = HostInitiator_295
      Host              = Host_40
      UID               = 50:01:43:80:24:D1:B7:C1:50:01:43:80:16:7D:A2:D4
      Ignored           = no
      Health Details    = "The initiator does not have any logged in initiator paths. Check the c
onnection between the initiator and the storage system.

2:    ID                = HostInitiator_296
      Host              = Host_40
      UID               = 50:01:43:80:24:D1:F9:99:50:01:43:80:16:7D:F2:64
      Ignored           = no
      Health Details    = "The initiator does not have any logged in initiator paths. Check the c
onnection between the initiator and the storage system.

3:    ID                = HostInitiator_337
      Host              = Host_40
      UID               = 50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18
      Ignored           = no
      Health Details    = "The component is operating normally. No action is required."

4:    ID                = HostInitiator_338
      Host              = Host_40
      UID               = 50:01:43:80:24:D1:B9:ED:50:01:43:80:16:7D:B2:38
      Ignored           = no
      Health Details    = "The component is operating normally. No action is required."
```

6. Deregister the old initiators from the faulty blade. The commands are as follows to remove each of the initiators that do not have any logged in initiators paths as identified in output from step 5.

   Using the example information from step 5, the commands are as follows:

```
[root@ms ~]# /usr/bin/uemcli -d 10.151.181.182 /remote/initiator -id HostInitiator_295 set -ignore
d yes
```

```
[root@ms ~]# /usr/bin/uemcli -d 10.151.181.182 /remote/initiator -id HostInitiator_295 set -host "
" -force
```

```
[root@ms ~]# /usr/bin/uemcli -d 10.151.181.182 /remote/initiator -id HostInitiator_296 set -ignore
d yes
```

```
[root@ms ~]# /usr/bin/uemcli -d 10.151.181.182 /remote/initiator -id HostInitiator_296 set -host "
" -force
```

7. Verify that the host is configured correctly by running the following commands:

   ```
   [root@ms]# [root@ms]# /usr/bin/uemcli -d <sp_ip> /remote/initiator -host Hos
   t_40 show -detail
   ```

   Example output is as follows:

   ```
   1:    ID                 = HostInitiator_337
         Host               = Host_40
         UID                = 50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18
         Initiator type     = fc
         Ports logged in    = spa_fc5,spa_iom_0_fc1,spa_iom_0_fc3,spa_fc4
         Ignored            = no
         Health State       = OK (5)
         Health Details     = "The component is operating normally. No action i
   s required."
         CHAP users         =
         Source type        = OpenNative
         Failover mode      = ALUA
         LUNZ enabled       = yes
         Unit serial number = Array

   2:    ID                 = HostInitiator_338
         Host               = Host_40
         UID                = 50:01:43:80:24:D1:B9:ED:50:01:43:80:16:7D:B2:38
         Initiator type     = fc
         Ports logged in    = spb_fc5,spb_fc4,spb_iom_0_fc3,spb_iom_0_fc1
         Ignored            = no
         Health State       = OK (5)
         Health Details     = "The component is operating normally. No action i
   s required."
         CHAP users         =
         Source type        = OpenNative
         Failover mode      = ALUA
         LUNZ enabled       = yes
         Unit serial number = Array
   ```

Results

SAN configuration for the replacement blade is updated.

5.13.7.10.2 Update VNX SAN Configuration for the Replacement Blade

> This task describes how to update the SAN configuration to enable the replacement blade to inherit the LUNs of the faulted blade.

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.

2. Use the following command to list the SP port information where <SAN_SP_IP_Address> represents the IP address of one of the SAN's SP ports.

   For the value of this IP address, refer to the *AMOS, Advanced MO Scripting, User Guide*.

```
[root@ms ~]# /opt/Navisphere/bin/naviseccli -h <SAN_SP_IP_Address> -user <US →
ER> -password <PASSWORD> -scope 0 port -list
```

   Example output:

```
...
...
Information about each HBA:

HBA UID:                 50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18
Server Name:             50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18
Server IP Address:       UNKNOWN
HBA Model Description:
HBA Vendor Description:
HBA Device Driver Name:
Information about each port of this HBA:

    SP Name:               SP A
    SP Port ID:            1
    HBA Devicename:
    Trusted:               NO
    Logged In:             YES
    Source ID:             1901824
    Defined:               NO
    Initiator Type:           3
    StorageGroup Name:     None

    SP Name:               SP B
    SP Port ID:            1
    HBA Devicename:
    Trusted:               NO
    Logged In:             YES
    Source ID:             1901824
    Defined:               NO
    Initiator Type:           3
    StorageGroup Name:     None


Information about each HBA:

HBA UID:                 50:01:43:80:24:D1:B9:ED:50:01:43:80:16:7D:B2:38
Server Name:             50:01:43:80:24:D1:B9:ED:50:01:43:80:16:7D:B2:38
Server IP Address:       UNKNOWN
HBA Model Description:
HBA Vendor Description:
HBA Device Driver Name:
Information about each port of this HBA:

    SP Name:               SP A
    SP Port ID:            3
    HBA Devicename:
    Trusted:               NO
    Logged In:             YES
    Source ID:             1967360
    Defined:               NO
    Initiator Type:           3
    StorageGroup Name:     None

    SP Name:               SP B
    SP Port ID:            3
    HBA Devicename:
    Trusted:               NO
    Logged In:             YES
    Source ID:             1967360
    Defined:               NO
    Initiator Type:           3
```

```
    StorageGroup Name:     None


Information about each HBA:

HBA UID:                 50:01:43:80:24:D1:B7:C1:50:01:43:80:16:7D:A2:D4
Server Name:             enmsvc1
Server IP Address:       10.47.142.108
HBA Model Description:
HBA Vendor Description:
HBA Device Driver Name:
Information about each port of this HBA:

    SP Name:               SP A
    SP Port ID:            3
    HBA Devicename:
    Trusted:               NO
    Logged In:             NO
    Defined:               YES
    Initiator Type:           3
    StorageGroup Name:     SANENM1-enm-svc_cluster-svc-1

    SP Name:               SP B
    SP Port ID:            3
    HBA Devicename:
    Trusted:               NO
    Logged In:             NO
    Defined:               YES
    Initiator Type:           3
    StorageGroup Name:     SANENM1-enm-svc_cluster-svc-1

Information about each HBA:

HBA UID:                 50:01:43:80:24:D1:F9:99:50:01:43:80:16:7D:F2:64
Server Name:             enmsvc1
Server IP Address:       10.47.142.108
HBA Model Description:
HBA Vendor Description:
HBA Device Driver Name:
Information about each port of this HBA:

    SP Name:               SP A
    SP Port ID:            1
    HBA Devicename:
    Trusted:               NO
    Logged In:             NO
    Defined:               YES
    Initiator Type:           3
    StorageGroup Name:     SANENM1-enm-svc_cluster-svc-1

    SP Name:               SP B
    SP Port ID:            1
    HBA Devicename:
    Trusted:               NO
    Logged In:             NO
    Defined:               YES
    Initiator Type:           3
    StorageGroup Name:     SANENM1-enm-svc_cluster-svc-1
...
...
```

In the previous example output, the initiators for the replacement blade are not assigned yet so they have the same value in the `HBA UID` and `Server Name` fields. The `Server IP Address` is set to `UNKNOWN`. The HBAs for the faulted blade in the previous example output have `Server Name` set to `enmsvc1` and `Server IP Address` set to `10.47.142.108`.

From the command output, record the following information, which is a combination of the information listed about the old and new hardware:

`HBA UID`, `SP Name`, `SP Port ID`, `StorageGroup Name`, `Server Name` and `Server IP Address`

Note: `StorageGroup Name`, `Server Name` and `Server IP Address` are common to all the commands run in step 3. The `HBA UID`, `SP Name` and `SP Port ID` are specific for the ports of each of the replacement blade HBAs, therefore, it is important that they are recorded together for individual commands in step 3.

The following table is populated from the previous example output. It contains specific information for the ports of each of the replacement blade HBAs:

HBA UID	SP Name	SP Port ID
50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18	A	1
50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18	B	1
50:01:43:80:24:D1:B9:ED:50:01:43:80:16:7D:B2:38	A	3
50:01:43:80:24:D1:B9:ED:50:01:43:80:16:7D:B2:38	B	3

The following table is populated from the previous example output. It contains the required common information:

Information Name	Values
StorageGroup Name	SANENM1-enm-svc_cluster-svc-1
Server Name	enmsvc1
Server IP Address	10.47.142.108

3. Register the initiators using the information from the tables in step 2 and run the following command for each entry, where `<Storage_Group_Name>`, `<HBA_UID>`, `<SP_Name>`, `<SP_Port_ID>`, `<Server_IP_Address>` and `<Server_Name>` are taken from the tables in step 2:

```
[root@ms ~]# naviseccli -h <SAN_SP_IP_Address> storagegroup /
-setpath -o -gname <Storage_Group_Name> /
-hbauid <HBA_UID> /
-sp <SP_Name> -spport <SP_Port_ID> -type 3 /
-ip <Server_IP_Address> -host <Server_Name> /
-failovermode 4 -arraycommpath 1
```

Using the example information from step 2, the commands are as follows:

```
[root@ms ~]# naviseccli -h 10.52.177.44 storagegroup /
-setpath -o -gname SANENM1-enm-svc_cluster-svc-1 /
-hbauid 50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18 /
-sp A -spport 0 -type 3 /
-ip 10.47.142.108 -host enmsvc1 /
-failovermode 4 -arraycommpath 1

[root@ms ~]# naviseccli -h 10.52.177.44 storagegroup /
-setpath -o -gname SANENM1-enm-svc_cluster-svc-1 /
-hbauid 50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18 /
-sp A -spport 1 -type 3 /
-ip 10.47.142.108 -host enmsvc1 /
-failovermode 4 -arraycommpath 1

[root@ms ~]# naviseccli -h 10.52.177.44 storagegroup /
-setpath -o -gname SANENM1-enm-svc_cluster-svc-1 /
-hbauid 50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18 /
```

```
-sp B -spport 0 -type 3 /
-ip 10.47.142.108 -host enmsvc1 /
-failovermode 4 -arraycommpath 1

[root@ms ~]# naviseccli -h 10.52.177.44 storagegroup /
-setpath -o -gname SANENM1-enm-svc_cluster-svc-1 /
-hbauid 50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18 /
-sp B -spport 1 -type 3 /
-ip 10.47.142.108 -host enmsvc1 /
-failovermode 4 -arraycommpath 1

[root@ms ~]# naviseccli -h 10.52.177.44 storagegroup /
-setpath -o -gname SANENM1-enm-svc_cluster-svc-1 /
-hbauid 50:01:43:80:24:D1:B9:ED:50:01:43:80:16:7D:B2:38 /
-sp A -spport 3 -type 3 /
-ip 10.47.142.108 -host enmsvc1 /
-failovermode 4 -arraycommpath 1

[root@ms ~]# naviseccli -h 10.52.177.44 storagegroup /
-setpath -o -gname SANENM1-enm-svc_cluster-svc-1 /
-hbauid 50:01:43:80:24:D1:B9:ED:50:01:43:80:16:7D:B2:38 /
-sp B -spport 3 -type 3 /
-ip 10.47.142.108 -host enmsvc1 /
-failovermode 4 -arraycommpath 1
```

4. Deregister the old HBAs:

    a. List the HBAs associated with the host where the value for <Storage_Group_Name> is taken from the table in step 3:

    ```
    [root@ms ~]# naviseccli -h <SAN_SP_IP_Address> storagegroup -list /
    -gname <Storage_Group_Name>
    ```

    Example output:

    ```
    [root@ms ~]# naviseccli -h 10.52.177.44 storagegroup -list /
    -gname SANENM1-enm-svc_cluster-svc-1

    Storage Group Name:    SANENM1-enm-svc_cluster-svc-1
    Storage Group UID:     GD:4E:25:55:7E:48:E6:11:2E:A6:00:60:85:3G:22 →
    :11
    HBA/SP Pairs:

      HBA UID                                          SP Name     SPPo →
    rt
      -------                                          -------     ---- →
    --
      50:01:43:80:24:D1:F9:99:50:01:43:80:16:7D:F2:64   SP A         1
      50:01:43:80:24:D1:B9:ED:50:01:43:80:16:7D:B2:38   SP A         3
      50:01:43:80:24:D1:F9:99:50:01:43:80:16:7D:F2:64   SP B         1
      50:01:43:80:24:D1:B9:ED:50:01:43:80:16:7D:B2:38   SP B         3
      50:01:43:80:24:D1:B7:C1:50:01:43:80:16:7D:A2:D4   SP A         3
      50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18   SP A         1
      50:01:43:80:24:D1:B7:C1:50:01:43:80:16:7D:A2:D4   SP B         3
      50:01:43:80:24:D1:F9:21:50:01:43:80:16:7D:B2:18   SP B         1

    HLU/ALU Pairs:

      HLU Number     ALU Number
      ----------     ----------
        1              7
        2              8
        0              9
    Shareable:             YES
    ```

    b. Record the HBA UIDs of the faulted blade:

HBA UID
50:01:43:80:24:D1:B7:C1:50:01:43:80:16:7D:A2:D4

HBA UID
50:01:43:80:24:D1:F9:99:50:01:43:80:16:7D:F2:64

c. Deregister the HBAs with the following command where value for <HBA_UID> is taken from step 5.b:

```
[root@ms ~]# naviseccli -h <SAN_SP_IP_Address> port -removeHBA /
-hbauid <HBA_UID>
```

Example output:

```
[root@ms ~]# naviseccli -h 10.52.177.44 port -removeHBA /
-hbauid 50:01:43:80:24:D1:B7:C1:50:01:43:80:16:7D:A2:D4

Remove HBA:            50:01:43:80:24:D1:F9:99:50:01:43:80:24:D1:F9 →
:98  (y/n)? y

[root@ms ~]# naviseccli -h 10.52.177.44 port -removeHBA /
-hbauid 50:01:43:80:24:D1:F9:99:50:01:43:80:16:7D:F2:64

Remove HBA:            50:01:43:80:24:D1:B7:C1:50:01:43:80:24:D1:B7 →
:C0  (y/n)? y
```

Results

SAN configuration for the replacement blade is updated.

5.13.7.11 Boot the Replacement Blade into Single User Mode

When the replacement blade is successfully registered on the SAN, return to the nodes iLO Console Session and boot the replacement blade into single user mode.

Steps

1. Log on to the iLO web manager of the replacement blade as an administrator user and open a console connection by selecting **Remote Console** > **Integrated Remote Console**.
2. From the Integrated Remote Console menu, select **Power Switch** > **Cold Boot**, wait for the GRUB splash screen to appear, and then press any key to enter the GRUB interactive menu.
3. From the GRUB interactive menu, select the OS that you want to boot.

   Note: If the blade that is being replaced belongs to a database node, select vxdmp_root from the GRUB menu. For all other nodes, select Red Hat Enterprise Linux.

   Press p and enter the password.

   Note: The GRUB interactive menu prompts for a password. If you do not know the password, then contact Ericsson support.
4. Press a to edit the kernel commands.

5. Remove the `console` parameter from the boot arguments.

   Example

   The following shows a section of the output from step 3 where `<console=ttyS0,115200>` is the argument to be removed.

   ```
   root rd_NO_DM rhgb quiet console=ttyS0,115200
   ```

6. Add `1` to the end of the boot arguments to specify a run level of 1.

   Example

   ```
   root rd_NO_DM rhgb quiet 1
   ```

7. Press `Enter` to boot.

   Note: You might receive a prompt `Please enter the root password or hit enter to continue`. If this appears, then enter the root password before continuing. If you do not know the password, then contact Ericsson support.

Results

Replacement blade is booted into single user mode.

5.13.7.12 Disable Puppet Agent on the Replacement Node

When you boot the node fully later in the procedure, make sure that LITP does not overwrite any configuration that was applied manually. To prevent LITP from overwriting the configuration, disable the Puppet agent on the replacement node.

Steps

1. Disable the Puppet agent:

   ```
   # puppet agent --disable
   ```

Results

Puppet agent is disabled.

5.13.7.13 Remove the Cached Catalog on the Replacement Node

To prevent the old configuration from being applied in the LITP plan, remove the cached catalog on the replacement node.

Steps

1. Remove the cached catalog:

```
# /bin/rm -f /var/lib/puppet/client_data/catalog/*
```

Results

Cached catalog is removed from the replacement node.

5.13.7.14 Update the Networking Files on the Replacement Blade

When the system is in single user mode, the next step is to update some networking files with the MAC addresses of the replacement blade. This prevents any issues with networking and VCS startup on the first boot of the replacement bade.

Note: Create backups of the networking files in the following sections before updating the files. This ensures that the files can be rolled back easily if you have to return the cluster to the original state.

Steps

1. Update the `udev` rule for `eth0` with the value of the Port 1 MAC address that you recorded in Retrieve MAC Addresses and Serial Number of the Replacement Blade.

   Note: The format of the recorded address might differ from the format required for the rules file.

MAC Address (VC)	MAC Address (udev)
A5-C2-17-3F-AC-E0	a5:c2:17:3f:ac:e0

   a. Back up the file:

```
# cp /etc/udev/rules.d/70-persistent-net.rules /etc/udev/rules.d/70 →
-persistent-net.rules_backup
```

   b. Edit the file:

```
# vi /etc/udev/rules.d/70-persistent-net.rules
```

   c. Update any `ATTR{address}` values for each interface with the corresponding MAC address of the replacement blade and then save the file.

      After editing, the file is similar to the following example:

```
# Generated by Cobbler

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*", ATTR{address}=="a5: →
c2:17:3f:ac:e0", ATTR{type}=="1", KERNEL=="eth*", NAME="eth0"
```

2. Update the network scripts for the `eth2` and `eth3` interfaces with the new MAC address values.

a. Back up the files:

```
# cp /etc/sysconfig/network-scripts/ifcfg-eth2 /etc/sysconfig/netwo →
rk-scripts/ifcfg-eth2_backup
# cp /etc/sysconfig/network-scripts/ifcfg-eth3 /etc/sysconfig/netwo →
rk-scripts/ifcfg-eth3_backup
```

b. Edit the files:

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth2
# vi /etc/sysconfig/network-scripts/ifcfg-eth3
```

c. For each of the files opened in step 2.b, set the `HWADDR` parameter for each interface to the new MAC address.

After editing, the files are similar to the following example:

```
DEVICE=eth2
USERCTL=no
NOZEROCONF=yes
ONBOOT=yes
HWADDR=A5:C2:17:3F:AC:E1
BOOTPROTO=static
```

```
DEVICE=eth3
USERCTL=no
NOZEROCONF=yes
ONBOOT=yes
HWADDR=A5:C2:17:3F:AC:E9
BOOTPROTO=static
```

3. Update the `/etc/llttab` file for interfaces `eth2` and `eth3`.

Note: This file is used by VCS for Heartbeat connections and must be updated with the new MAC address of the replacement blade.

a. Back up the files:

```
# cp /etc/llttab /etc/llttab_backup
```

b. Edit the file:

```
# vi /etc/llttab
```

c. Modify the file so that the entries for `eth2` and `eth3` are set to their correct MAC addresses.

After editing, the file contains two lines, similar to the following example:

```
...
...
link eth3 eth3-A5:C2:17:3F:AC:E9 - ether - -
link eth2 eth2-A5:C2:17:3F:AC:E1 - ether - -
....
~
```

Results

The following networking files are updated:

— `Udev` rules file

— Network scripts

— `/etc/lltab` file

5.13.7.15 Exit from Single User Mode

The following steps provide instructions about how to exit from single user mode, boot the node and make it contactable.

Steps

1. Restart the replacement node and wait for the reboot to complete:

   ```
   # shutdown -r now
   ```

2. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.

3. Enter the following command to verify that the replacement node is fully up and contactable where `<node name>` represents the name of the node.

   ```
   [root@ms]# mco ping -I <node name>
   ```

   Example output:

   ```
   node                                time=27.05 ms

   ---- ping statistics ----
   5 replies max: 27.05 min: 24.88 avg: 25.99
   ```

Note: If mco ping is not successful for the replacement blade and returns with "No responses received", check to ensure the swclock and hwclock are correct on all the replacement blades. On the MS get the current time and date, with the date command.

```
# date
```

Log on as the *root* user to the iLO of the replacement blade and check the date and time, if they are not the same as on the MS, then it should be set to align with the time on the MS and the swclock and hwclock should be synced on all the replacement blades using the following commands.

```
# date +%T -s "<time>"
```

```
# hwclock --systohc
```

The date and time are now in sync on all replacement blades.

4. Repeat step 3 to verify that the replacement node is fully up and contactable.

Results

Replacement node is fully operational and contactable.

5.13.7.16 Unlock the Replacement Node of the Cluster

Unlock the replacement node to bring it back into the cluster and bring services online before running the LITP plan.

Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. Unlock the replacement node and bring services back online by entering the following command, where `<node name>` is the name of the frozen node seen in the output of the `hastatus -sum` command.

```
[root@ms ~]# mco rpc vcs_cmd_api unlock sys=<node name> nic_wait_timeout=120 →
 -I <node name>
```

3. Verify that the node is no longer frozen and that all relevant services for that node are online.
    a. Log on as the `litp-admin` user from the ENM MS to the replacement node and switch to the `root` user:

```
[litp-admin@node-2 ~]$ su -
```

b. Check the cluster status:

```
[root@node-2 ~]# hastatus -sum
```

Results

The replacement node is unlocked and all relevant services for that node are online

5.13.7.17 Update the LITP Model on the ENM MS

When the replacement node is operational and contactable, complete the following steps to update the LITP model.

Steps

1. Update the existing node `macaddress` property items in the LITP model to the values of the replacement blade.

    a. Log on as the `litp-admin` user to the ENM MS.

    b. Record the original MAC address values from the LITP model in case they are required for rollback, using commands similar to the following where `<cluster>` and `<node_name>` represent the values for the cluster type and name of the node:

```
[litp-admin@ms ~]$ litp show -p /deployments/enm/clusters/<cluster> →
/nodes/<node_name>/network_interfaces/eth0
[litp-admin@ms ~]$ litp show -p /deployments/enm/clusters/<cluster> →
/nodes/<node_name>/network_interfaces/eth1
[litp-admin@ms ~]$ litp show -p /deployments/enm/clusters/<cluster> →
/nodes/<node_name>/network_interfaces/eth2
[litp-admin@ms ~]$ litp show -p /deployments/enm/clusters/<cluster> →
/nodes/<node_name>/network_interfaces/eth3
```

    c. Update the LITP model `macaddress` properties with the new MAC addresses of this node using commands similar to the following where`<cluster>` and `<node_name>` are variables and need to be updated depending on the cluster type and name of the node.

```
[litp-admin@ms ~]$ litp update -p /deployments/enm/clusters/<cluste →
r>/nodes/<node_name>/network_interfaces/eth0 -o macaddress="A5:C2:1 →
7:3F:AC:E0"
[litp-admin@ms ~]$ litp update -p /deployments/enm/clusters/<cluste →
r>/nodes/<node_name>/network_interfaces/eth1 -o macaddress="A5:C2:1 →
7:3F:AC:E8"
[litp-admin@ms ~]$ litp update -p /deployments/enm/clusters/<cluste →
r>/nodes/<node_name>/network_interfaces/eth2 -o macaddress="A5:C2:1 →
7:3F:AC:E1"
[litp-admin@ms ~]$ litp update -p /deployments/enm/clusters/<cluste →
r>/nodes/<node_name>/network_interfaces/eth3 -o macaddress="A5:C2:1 →
7:3F:AC:E9"
```

2. Update the LITP model with the WWPN addresses of the replacement blade:

a. Record the original MAC address values from the LITP model, in case they are required for rollback using commands similar to the following where <system_name> represents the system associated with the node:

```
[litp-admin@ms ~]$ litp show -p /infrastructure/systems/<system_nam →
e>/controllers/hba1
[litp-admin@ms ~]$ litp show -p /infrastructure/systems/<system_nam →
e>/controllers/hba2
```

b. Update each hba_porta_wwn parameter with the values for the replacement blades, using commands similar to the following where <system_name> represents the system associated with the node.

```
[litp-admin@ms ~]$ litp update -p /infrastructure/systems/<system_n →
ame>/controllers/hba1 -o hba_porta_wwn="50:01:43:80:16:7d:b2:18"
[litp-admin@ms ~]$ litp update -p /infrastructure/systems/<system_n →
ame>/controllers/hba2 -o hba_porta_wwn="50:01:43:80:16:7d:b2:38"
```

Note: Record the original hba_porta_wwn values, in case they are required for rollback.

3. Create and run the LITP plan:

   a. Switch back to the litp-admin user on the ENM MS.

   b. Configure the changes made to the LITP model and run the LITP plan:

```
[litp-admin@ms ~]$ litp create_plan
[litp-admin@ms ~]$ litp run_plan
```

   c. Monitor the progress of the LITP plan:

```
[litp-admin@ms ~]$ watch litp show_plan
```

Results

LITP model is updated

5.13.7.18 Check Cluster Status

When the LITP model is updated, check that all the expected services are online.

Steps

1. Log on to a node in the cluster and switch to the root user:

```
[litp-admin@node-2 ~]$ su -
```

2. Check the cluster status:

```
[root@node-2 ~]# hastatus -sum
```

Results

Services are online.

5.13.7.19 Check the Status of the Puppet Agent on the Replacement Node

After checking the status of the cluster, verify that the Puppet agent is running on the replacement node.

Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. Enter the following command to verify that the Puppet agent is enabled and fully running on the replacement node, where `<node name>` represents the name of the node.

```
[root@ms ~]#  mco puppet status -I <node name>
```

Results

Puppet agent is enabled and running.

5.13.7.20 Perform Post Replacement Tasks

When the blade replacement is completed successfully, perform the following steps.

The SED document still contains information related to the faulted blade, such as the serial number, MAC Addresses and WWPNs. You must update these values to reflect the values of the replacement blade.

Steps

1. Update the SED file with the serial number, MAC addresses and WWPNs of the replacement blade.

   An example of the SED parameters to update is as follows:

```
svc_node1_eth0_macaddress=A5:C2:17:3F:AC:E0
svc_node1_eth1_macaddress=A5:C2:17:3F:AC:C8
svc_node1_eth2_macaddress=A5:C2:17:3F:AC:C1
svc_node1_eth3_macaddress=A5:C2:17:3F:AC:C9
svc_node1_WWPN1=50:01:43:80:16:7d:b2:18
svc_node1_WWPN2=50:01:43:80:16:7d:b2:38
svc_node1_vcProfile=ENM_SE_db_node-1
svc_node1_serial=CZ351S3T2P
```

2. Perform *Update ENM Backup Policies* from ENM Backup and Restore System Administrator Guide [15] to add the BRS and NetBackup Configuration to the replacement blade.
3. Perform a backup of the ENM deployment with the replacement blade.

   For more information, refer to the ENM Installation Instructions.

Results

— SED document updated with the replacement blade information

— ENM backup performed

5.13.8 Rack Peer Node Hardware Replacement

Use this procedure to replace a faulted peer node on a HPE rack server in use in an ENM cluster.

Prerequisites

— There is no failed LITP plan in place.

— Administrator access to the ENM MS and managed nodes.

— Root Access on the faulted rack.

— Cluster name and node ID of the faulted rack from the LITP deployment model

— Access to the following information for the new rack server

  — UUID

  — MAC addresses for each interface

  — iLO IP address

Required Tools and Equipment

— The replacement rack server has the same characteristics as the faulted rack server, including HBA and NIC cards, and is part of the same subnet.

Steps

1. Ensure the rack server to be replaced is powered off by following the instructions in the ENM Power Down Procedure on page 24.
2. Refer to the following sections in the ENM Installation Instructions for details on how to prepare the new rack server for installation:

Table 4 Installation Stages

Stage	Section
Ethernet cabling	Connect Gen10 or Gen9 Streaming Cluster Rack to Ethernet
Firmware upgrades/downgrades	Firmware Overview
ILO configuration	Configure the iLO IP Address
ILO Licenses	Add iLO Licenses to HPE ProLiant Rack Servers
BIOS Procedures	Gen10 Rack Server BIOS Procedure or Gen9 Rack Server BIOS Procedure

3. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
4. Set the node to `Initial` in the LITP deployment model by running the following command:

```
[root@ms-1 ~]# litp prepare_restore -p /deployments/enm/clusters/<cluster_na →
me>/nodes/<node_id>
```

5. Update the LITP deployment model with the `UUID` from the new rack server:

```
[root@ms-1 ~]# litp update -p /deployments/enm/clusters/<cluster_name>/nodes →
/<node_id>/system/disks/boot_disk -o uuid=<uuid>

[root@ms-1 ~]# litp update -p /infrastructure/systems/<node_id>_system/disks →
/boot_disk -o uuid=<uuid>
```

6. Update the LITP deployment model with the MAC addresses for the new rack server:

```
[root@ms-1 ~]# litp update -p /deployments/enm/clusters/<cluster_name>/nodes →
/<node_id>/network_interfaces/eth0 -o macaddress=<eth0_MAC_address>

[root@ms-1 ~]# litp update -p /deployments/enm/clusters/<cluster_name>/nodes →
/<node_id>/network_interfaces/eth1 -o macaddress=<eth1_MAC_address>

[root@ms-1 ~]# litp update -p /deployments/enm/clusters/<cluster_name>/nodes →
/<node_id>/network_interfaces/eth2 -o macaddress=<eth2_MAC_address>

[root@ms-1 ~]# litp update -p /deployments/enm/clusters/<cluster_name>/nodes →
/<node_id>/network_interfaces/eth3 -o macaddress=<eth3_MAC_address>

[root@ms-1 ~]# litp update -p /deployments/enm/clusters/<cluster_name>/nodes →
/<node_id>/network_interfaces/eth4 -o macaddress=<eth4_MAC_address>

[root@ms-1 ~]# litp update -p /deployments/enm/clusters/<cluster_name>/nodes →
/<node_id>/network_interfaces/eth5 -o macaddress=<eth5_MAC_address>

[root@ms-1 ~]# litp update -p /deployments/enm/clusters/<cluster_name>/nodes →
/<node_id>/network_interfaces/eth6 -o macaddress=<eth6_MAC_address>
```

7. Update the LITP deployment model with the iLO address for the new rack server:

```
[root@ms-1 ~]# litp update -p /deployments/enm/clusters/<cluster_name>/nodes
/<node_id>/system/bmc -o ipaddress=<iLO_IP_address>
```

8. Create the LITP plan:

```
[root@ms-1 ~]# litp create_plan
```

9. Run the LITP plan :

```
[root@ms-1 ~]# litp run_plan
```

10. When the plan starts, it is possible to monitor the progress in a separate terminal instance using the following commands:

```
[root@ms-1 ~]# cd /opt/ericsson/enminst/bin/
[root@ms-1 bin]# ./monitor_plan.sh
```

11. Update the Site Engineering Document with the `MAC` address, `iLO IP` address, `UUID` and the hostname of the new rack server.

5.13.9 List ENM Firmware Levels

> This section describes the procedure to list the firmware levels in an ENM deployment.

Prerequisites

— ENM is deployed on the hardware.

— The *ENM Site Engineering Document (SED)* is available.

— Password for the `litp-admin` account of the ENM servers.

Steps

1. Generate a SED text file using the ENM SED.
2. Upload the text file to the `/var/tmp` directory of the ENM Management Server (MS). Subsequent steps refer to this text file as `<sed text file>`.
3. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.

4. List the current hardware firmware levels by running the following command:

```
[root@ms]# /opt/ericsson/hw_comm/bin/hw_comm.sh check_firmware /var/tmp/<sed →
 text file>
```

Enter the `litp-admin` password for the ENM peer servers when prompted.

Output example:

```
INFO: Firmware information for the deployment defined in SED:
=====================================================
enclosure1 ieatc7000-123 and blade firmware information
=====================================================

Enclosure firmware information
Bay  Type     Firmware
----------------------
OA1  OA       4.50
OA2  OA       4.50
1    VC       4.45
2    VC       4.45
3    Brocade  7.3.0c
5    Brocade  7.3.0c

Blade Firmware information
Bay  Node       Model/Gen    iLO         System ROM      NIC
-------------------------------------------------------------------
4    db_node1   BL460c Gen9  iLO 4 2.30  I36 09/24/2015  bc 7.12.83
5    svc_node1  BL460c Gen9  iLO 4 2.30  I31 06/01/2015  bc 7.12.83
6    svc_node3  BL460c Gen9  iLO 4 2.30  I31 06/01/2015  bc 7.12.83

=====================================================
enclosure2 ieatc7000-124 and blade firmware information
=====================================================

Enclosure firmware information
Bay  Type     Firmware
----------------------
OA1  OA       4.50
OA2  OA       4.50
1    VC       4.45
2    VC       4.45
3    Brocade  7.3.0c
5    Brocade  7.3.0c

Blade Firmware information
Bay  Node       Model/Gen    iLO         System ROM      NIC
-------------------------------------------------------------------
4    db_node2   BL460c Gen9  iLO 4 2.30  I36 09/24/2015  bc 7.12.83
5    svc_node2  BL460c Gen9  iLO 4 2.30  I31 06/01/2015  bc 7.12.83
6    svc_node4  BL460c Gen9  iLO 4 2.30  I31 06/01/2015  bc 7.12.83

=========================
Rack firmware information
=========================

LMS Firmware Information
Node  Model/Gen   iLO         System ROM      Smart Array
-----------------------------------------------------------
LMS   DL360 Gen9  iLO 4 2.30  P89 07/20/2015  P440ar 3.00

LMS (ms-1) NIC Firmware and Driver Info
Interface  Firmware Version           Driver  Driver Version
-----------------------------------------------------------
eth0       0x80000811                 ixgbe   3.19.1-k
eth1       0x80000811                 ixgbe   3.19.1-k
eth2       0x80000811                 ixgbe   3.19.1-k
eth3       0x80000811                 ixgbe   3.19.1-k
eth4       5719-v1.42 NCSI v1.3.12.0  tg3     3.137
eth5       5719-v1.42 NCSI v1.3.12.0  tg3     3.137
eth6       5719-v1.42 NCSI v1.3.12.0  tg3     3.137
eth7       5719-v1.42 NCSI v1.3.12.0  tg3     3.137
```

```
PEER RACK node Firmware Information
Node       Model/Gen   iLO         System ROM      Smart Array
-------------------------------------------------------------------
str_node1  DL380 Gen9  iLO 4 2.30  P89 07/20/2015  P440ar 3.56
str_node2  DL380 Gen9  iLO 4 2.30  P89 12/27/2015  P440ar 3.56

PEER RACK (str_node1) (ieatrcx6503) NIC Firmware and Driver Info
Interface  Firmware Version          Driver  Driver Version
-----------------------------------------------------------
eth0       5719-v1.38 NCSI v1.3.5.0  tg3     3.137
eth1       5719-v1.38 NCSI v1.3.5.0  tg3     3.137
eth2       5719-v1.38 NCSI v1.3.5.0  tg3     3.137
eth3       5719-v1.38 NCSI v1.3.5.0  tg3     3.137
eth4       5719-v1.38 NCSI v1.3.5.0  tg3     3.137
eth5       5719-v1.38 NCSI v1.3.5.0  tg3     3.137
eth6       5719-v1.38 NCSI v1.3.5.0  tg3     3.137
eth7       5719-v1.38 NCSI v1.3.5.0  tg3     3.137
eth8       0x80000811                ixgbe   3.19.1-k
eth9       0x80000811                ixgbe   3.19.1-k

PEER RACK (str_node2) (ieatrcx6504) NIC Firmware and Driver Info
Interface  Firmware Version           Driver  Driver Version
------------------------------------------------------------
eth0       5719-v1.45 NCSI v1.3.12.0  tg3     3.137
eth1       5719-v1.45 NCSI v1.3.12.0  tg3     3.137
eth2       5719-v1.45 NCSI v1.3.12.0  tg3     3.137
eth3       5719-v1.45 NCSI v1.3.12.0  tg3     3.137
eth4       5719-v1.45 NCSI v1.3.12.0  tg3     3.137
eth5       5719-v1.45 NCSI v1.3.12.0  tg3     3.137
eth6       5719-v1.45 NCSI v1.3.12.0  tg3     3.137
eth7       5719-v1.45 NCSI v1.3.12.0  tg3     3.137
eth8       0x80000897                 ixgbe   3.19.1-k
eth9       0x80000897                 ixgbe   3.19.1-k


NAS Firmware Information
Node       Model/Gen    iLO         System ROM      Smart Array
-------------------------------------------------------------------
sfs_node1  DL380p Gen8  iLO 4 2.30  P70 07/01/2015  P420i 6.68
sfs_node2  DL380p Gen8  iLO 4 2.30  P70 07/01/2015  P420i 6.68

NAS sfs_node1 (sfs_01) NIC Firmware and Driver Info
Interface  Firmware Version           Driver  Driver Version
------------------------------------------------------------
pubeth0    3.2-9                      igb     3.4.7
pubeth1    3.2-9                      igb     3.4.7
pubeth2    3.2-9                      igb     3.4.7
pubeth3    5719-v1.34 NCSI v1.2.19.0  tg3     3.122q
pubeth4    5719-v1.34 NCSI v1.2.19.0  tg3     3.122q
pubeth5    5719-v1.34 NCSI v1.2.19.0  tg3     3.122q
priveth0   5719-v1.34 NCSI v1.2.19.0  tg3     3.122q
priveth1   3.2-9                      igb     3.4.7

NAS sfs_node2 (sfs_02) NIC Firmware and Driver Info
Interface  Firmware Version           Driver  Driver Version
------------------------------------------------------------
pubeth0    3.2-9                      igb     3.4.7
pubeth1    3.2-9                      igb     3.4.7
pubeth2    3.2-9                      igb     3.4.7
pubeth3    5719-v1.34 NCSI v1.2.19.0  tg3     3.122q
pubeth4    5719-v1.34 NCSI v1.2.19.0  tg3     3.122q
pubeth5    5719-v1.34 NCSI v1.2.19.0  tg3     3.122q
priveth0   5719-v1.34 NCSI v1.2.19.0  tg3     3.122q
priveth1   3.2-9                      igb     3.4.7

========================
SAN firmware information
========================

VNX Firmware Information
Name          Model    OE Revision
-------------------------------------
vnx123        VNX5400  05.33.008.5.119
```

Note: To determine what NAS solution is used, log on to the console IP of the NAS cluster as the `support` user. The first line of the banner message contains the name of the NAS solution being used.

5. Remove the SED text file:

```
[root@ms]# rm /var/tmp/<sed text file>
```

Results

The firmware levels in the ENM deployment are listed.

5.13.10 NAS Hardware Maintenance

This section contains topics on how to prepare the NAS hardware for maintenance activities, e.g. a firmware update, where the NAS node needs to be removed from the cluster.

— For a VA NAS follow Prepare NAS Hardware for Maintenance on page 80.

It also contains topics relating to the general administration of the NAS cluster, and topics that should be performed as part of a specific procedure e.g. a NAS restore or a NAS migration.

5.13.10.1 Prepare NAS Hardware for Maintenance

Before performing a maintenance procedure (for example, an update) on the NAS hardware you must first remove the hardware from the cluster. After performing the maintenance, return the hardware back into the deployment. Apply the updates to the slave node first and then to the master node.

Prerequisites

— NAS is available for updates.

— No deployment is in progress during this procedure.

— You have `support` access to the NAS.

Steps

1. Log on to the NAS management console as the `support` user and run the audit script.

```
# /opt/ericsson/NASconfig/bin/nasAudit.py
```

The script creates a HTML results file (with the following filename format), `/home/support/audit_report/NAS_Audit_<clustername>_<date_time>.html`.

Note: Before proceeding with maintenance procedures, correct any issues identified by the audit.

2. Identify the slave node in the cluster.

```
nas_01:~ # vxclustadm nidmap
Name                             CVM Nid    CM Nid     State
nas_01                              0          0          Joined: Master
nas_02                              1          1          Joined: Slave
nas_01:~ #
```

   In this example, the hostname of the slave node is `nas_02`.

3. Log on to the iLO of the master node as an `Administrator` user and launch the Remote Console.

4. From the Remote Console, log on as the `support` user, change user to `master` and shut down the slave node.

   Example

```
# su - master
nas_01> cluster shutdown nas_02
```

5. Before making the NAS available for the hardware update, verify that the VIPs have failed over to the master node.

```
nas_01> network ip addr show

IP            Netmask/Prefix  Device     Node    Type     Status
--            --------------  ------     ----    ----     ------
10.42.235.105 255.255.252.0   bond0      nas_01  Physical
10.42.235.106 255.255.252.0   bond0      nas_02  Physical
10.42.235.117 255.255.252.0   bond0      nas_01  Virtual  ONLINE (Con IP)
10.42.235.118 255.255.252.0   bond0      nas_01  Virtual  ONLINE
10.42.235.119 255.255.252.0   bond0      nas_01  Virtual  ONLINE
```

   The hardware is now available for maintenance update.

6. When the hardware is updated, power on the slave node and verify the node has rejoined the cluster.

7. Log on to the master node as the `support` user.

```
# hastatus -sum
```

8. Promote the slave to master by rebooting the master node.

```
nas_01> cluster reboot <master_node_name>
```

   Example

```
nas_01> cluster reboot nas_01
```

9. Verify that an equal amount of VIPs are on each node (excluding Con IP):

```
nas_02> network ip addr show

IP            Netmask/Prefix  Device     Node    Type     Status
--            --------------  ------     ----    ----     ------
10.42.235.105 255.255.252.0   bond0      nas_01  Physical
10.42.235.106 255.255.252.0   bond0      nas_02  Physical
10.42.235.117 255.255.252.0   bond0      nas_02  Virtual  ONLINE (Con IP)
10.42.235.118 255.255.252.0   bond0      nas_02  Virtual  ONLINE
10.42.235.119 255.255.252.0   bond0      nas_01  Virtual  ONLINE

nas_02> cluster show

Node        State      CPU(15 min)     bond0(15 min)
                            %        rx(MB/s) tx(MB/s)
----        -----      -----------   -------- --------
nas_01      RUNNING          4.04       0.00     0.00
nas_02      RUNNING          4.35       0.01     0.00
```

Repeat steps 2 to 7 on the second NAS node.

10. When the hardware is updated on both nodes, log on to the NAS management console as the `support` user.

11. Run the audit script to verify there are no errors in the cluster:

    ```
    # /opt/ericsson/NASconfig/bin/nasAudit.py
    ```

12. Post NAS reboot, update the `CLIENT_NAME` field of the `bp.conf` file with it's respective physical hostname.

    a. Log on to the ENM MS as the brsadm user:

    ```
    # ssh -X -l brsadm <ms ip address>
    ```

    b. Get the list of nodes connected to MS:

    ```
    # /opt/ericsson/itpf/bur/bin/bos --operation list_nodes
    ```

    Example:

    ```
    [brsadm@ieatlmsxxx-1 root]$ /opt/ericsson/itpf/bur/bin/bos --operat →
    ion list_nodes

    Node: db-1 Hostname: ieatrcxb2447 IP address: 10.247.246.5 Backup I →
    P: 10.151.24.72 Backup hostname:ieatrcxb2447-bkp1

    Node: db-2 Hostname: ieatrcxb3031 IP address: 10.247.246.8 Backup I →
    P: 10.151.24.75 Backup hostname: ieatrcxb3031-bkp1

    Node: svc-1 Hostname: ieatrcxb3049 IP address: 10.247.246.24 Backup →
     IP: 10.151.24.73 Backup hostname: ieatrcxb3049-bkp1

    Node: svc-2 Hostname: ieatrcxb3050 IP address: 10.247.246.25 Backup →
     IP: 10.151.24.74 Backup hostname: ieatrcxb3050-bkp1

    Node: svc-3 Hostname: ieatrcxb2563 IP address: 10.247.246.3 Backup  →
    IP: 10.151.24.70 Backup hostname: ieatrcxb2563-bkp1

    Node: svc-4 Hostname: ieatrcxb2564 IP address: 10.247.246.4 Backup  →
    IP: 10.151.24.71 Backup hostname: ieatrcxb2564-bkp1

    Node: nas VIP IP address: 10.140.59.110 Hostname: ieatsfsx422-423mg →
    t NAS Type: VA
    ```

```
Node: nas atsfsx422423_01 IP address: 10.140.59.106 Hostname: ieats →
fsx422-ph1

Node: nas atsfsx422423_02 IP address: 10.140.59.107 Hostname: ieats →
fsx423-ph1

Node: ms Hostname: ieatlmsxxx-1 IP address: 10.247.246.2 Backup IP: →
 10.151.24.149 Backup hostname: ieatlmsxxx-1-bkp1
```

c. Take note of the respective NAS physical hostnames from this list.

d. Log on to each NAS client and update the `CLIENT_NAME` field of the `/usr/openv/netbackup/bp.conf` file with it's respective physical hostname.

Results

NAS is made available for maintenance and returned to the deployment after the maintenance update.

5.13.10.2 Configure an Internal Network Interface on Veritas Access NAS for Routing of Mail

The section describes the tasks required to configure a network interface on the internal VLAN. The use case for this procedure is limited at this time to facilitating a connection to the ENM central email relay. It should not be used for any other purpose. The steps to configure forwarding of email from the NAS to the ENM mail relay is beyond the scope of this procedure.

This is an optional task and is applicable for both nodes in the Veritas Access deployment. It is performed using support user after installation of the VA NAS cluster.

Prerequisites

— NAS is installed and configured with Access NAS Configuration Kit.

— The installation IP addresses used to install the NAS cluster are known.

— The 1Gb links used for installation of the VA NAS cluster are still cabled as per the *Network and Storage Cabling* section of the ENM Installation Instruction.

— Login credentials to the Veritas Access NAS as `support` user are known.

Steps

1. Log on to the management console as `support` user and prepare the network interface on this node.
2. Identify the correct interface to configure.
    a. Log on to the iLO as Administrator using SSH.

b. Run the following command

```
</>hpiLO-> show /system1/network1/integrated_NICs
```

Example

```
hpiLO-> show /system1/network1/integrated_NICs
status=0
status_tag=COMMAND COMPLETED
Wed Oct 17 08:03:19 2018

/system1/network1/integrated_NICs
Targets
Properties
iLO4_MACAddress=50:65:f3:66:bc:16
Port1NIC_MACAddress=28:80:23:a6:8a:54
Port2NIC_MACAddress=28:80:23:a6:8a:55
Port3NIC_MACAddress=28:80:23:a6:8a:56
Port4NIC_MACAddress=28:80:23:a6:8a:57
Verbs
cd version exit show
```

c. Identify MAC address of installation interface.

i. For Gen10 or a Gen9 server, note the MAC address on port 1 of the adapter.

ii. For a Gen8 server, note the MAC address on port 2 of the adapter.

d. Log out of the iLO CLI.

e. As the support user on the management console, run the `ip link show` command, find the MAC address noted in the previous step and note the interface name for the MAC address.

```
# ip link show | more
```

3. Configure the network configuration file of the interface identified in the step above.

```
# vim /etc/sysconfig/network-scripts/ifcfg-<interface
```

4. Make sure the following parameters are set inthe file:

```
DEVICE=<interface>
BOOTPROTO=none
HWADDR=<hardware address>
IPADDR=<ip address>
NETMASK=<Netmask>
NM_CONTROLLED=no
ONBOOT=yes
```

where:

<interface> is the network interface identified in the previous step.

<hardware address>

is the MAC address of the interface identified in the previous step.

<ip address> is the extra internal IP address. The installation IP address used to install this NAS node must be re-used here.

<netmask is the Subnet Netmask IP address.

5. Save and exit the file.
6. Enter the following command to activate the interface:

```
# ifup <interface
```

7. Check that the interface can reach the gateway using the following command, where <interface> represents the 1Gb NIC selected at the beginning of this step and `<GATEWAY IP>` is the internal IP address of the ENM MS.

```
# ping -I <interface> -c 4 <GATEWAY IP>
```

8. Repeat the above steps on the second VA node, using the appropriate values for that node.

Results

A network interface is configured on the internal network for each VA node to allow emails to be relayed from the NAS to ENM.

5.13.10.3 Manual Backup of NAS Configuration and Metadata

This topic describes how to manually backup the NAS configuration and metadata if your site security policy prevents automated backup of the NAS configuration. The NAS configuration and metadata are archived on the ENM MS to keep a confirmed working configuration of the NAS that can be used for restoration.

Prerequisites

— `Root` user access to the ENM MS.

— `Support` user access to the NAS management console.

— `Master` user access to the CLISH.

— NAS is installed and configured with Access NAS Configuration Kit or SFS Configuration Kit.

— ENM MS IP address.

Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. Create the following directory if it does not already exist.

```
# mkdir /var/www/nasbackups
```

3. Log on to the NAS management console as `support` user.
4. Log on to the CLISH as `master` user.

```
# su - master
```

5. Make a backup of the NAS configuration and transfer the backup to the ENM MS. Enter the `root` password for the ENM MS when prompted.

```
nas> system config export remote scp://root@<ENM_MS_IP_Address>:/var/www/nas →
backups/<cluster name>-<YYYY-MM-DD>-Installed
```

6. Log out as the `master` user.

```
nas> logout
```

7. As `support` user, backup the NAS metadata to a file.
   a. If you are using SFS, please use this command.

```
# /opt/ericsson/SFSconfig/bin/fs_recovery.sh -a extract -m <metadata fi →
le path>
```

   b. If you are using VA, please use this command.

```
# /opt/ericsson/NASconfig/bin/fs_recovery.sh -a extract -m <metadata fi →
le path>
```

8. Copy the metadata file to the backup file location.

```
# scp <metadata file path> root@<ENM_MS_IP_Address>:/var/www/nasbackups/<clu →
ster name>-<YY-MM-DD>-Metadata
```

Results

A backup copy of the NAS configuration and metadata is created and exported to the ENM MS.

5.13.10.4 Add Node_02 to VA Cluster

This topic describes how to add the node to the VA cluster.

Prerequisites

— `root` user access to the VA nodes.

— `RHEL` has been installed on the node.

— The `RHEL` patches have been installed on the node.

— `WWN` of the node is added to the VA storage group.

Steps

1. Log on to the serial console of the existing Veritas Access node:

```
# ssh <va_iLo_admin>@<va_iLo_ip>
</>hpiLO-> start /system1/oemhp_vsp1
```

Note: If you are prevented from starting the session because another VSP session is running, it can be stopped using the following command.

```
</>hpiLO-> stop /system1/oemhp_vsp1
```

If logging on to VA iLo via SSH, do not initiate the SSH session while logged into the VA management console.

2. When prompted, enter the credentials for `master` user, to enter `clish`:

3. Add the node to the VA cluster using the '172.16.0.99' IP address:

```
nas> cluster add 172.16.0.99
```

If requested, enter the root password of the NAS node to set up SSH when prompted.

Note: A reboot will occur.

After the Veritas Access installation is complete, the following messages appear on the iLO remote console. These messages have no effect on the cluster and can be ignored.

```
vxdmpadm: Unknown error 4294967295

VxVM vxdisk ERROR V 5-1-558 Disk <hostname>_<node>_disk_0: Disk not →
 in the configuration

VxVM vxdisk ERROR V-5-1-531 Device <hostname>_<node>_disk_0: online →
 failed: Bad record name
```

4. Verify the reboot has started:

```
# su - master
> cluster show
Node State CPU(15 min) bond0(15 min)
 % rx(MB/s) tx(MB/s)
---- ----- ----------- -------- --------
node_01 EXITED
node_02 RUNNING 13.32 11.19 18.02
```

5. Verify the node has rejoined to the cluster (this can take 5-10 minutes):

```
> cluster show
Node State CPU(15 min) bond0(15 min)
 % rx(MB/s) tx(MB/s)
---- ----- ----------- -------- --------
node_01 RUNNING 3.42 1.50 3.72
node_02 RUNNING 13.32 11.19 18.02
```

6. Verify the VIPs are balanced by repeatedly running the following command until balanced:

```
> network ip addr show
IP Netmask/Prefix Device Node Type Status
-- -------------- ------ ---- ---- ------
10.1.1.2 255.255.252.0 bond0 nas551011_01 Physical
10.1.1.3 255.255.252.0 bond0 nas551011_02 Physical
10.1.1.10 255.255.252.0 bond0 nas551011_01 Virtual ONLINE (Co →
n IP)
10.1.1.11 255.255.252.0 bond0 nas551011_02 Virtual ONLINE
10.1.1.12 255.255.252.0 bond0 nas551011_01 Virtual ONLINE
```

Note: `rport` messages may appear. These messages have no effect on the cluster and can be ignored.

```
rport-X:X-XX: blocked FC remote port timeout: removing port
```

7. Log on to the added node as support user.

   a. Check whether the temporary `IP` still exists on the Installation NIC (eth<XX> can be identified from Step 21 of Install RHEL OS on page 122.

      Note: If the temporary `IP` is not configured then proceed to Step 8

      ```
      # ifconfig -a eth<XX>
      ```

      Example

      ```
      nas29342936_02:~ # ifconfig -a eth1
      eth1      Link encap:Ethernet  HWaddr AC:16:2D:70:3E:BD
                inet addr:10.42.235.128  Bcast:10.42.235.255  Mask:255.25 →
      ```

```
5.252.0
          inet6 addr: fe80::ae16:2dff:fe70:3ebd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6919 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:579845 (566.2 KiB)  TX bytes:1020 (1020.0 b)
          Interrupt:36
```

b. If the temporary IP still exists on the NIC , then open the following file to edit the contents:

```
# vim /etc/sysconfig/network-scripts/ifcfg-eth<XX>
```

Example

```
nas29342936_02:~ # vim /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
HWADDR=AC:16:2D:70:3E:BD
TYPE=Ethernet
UUID=667e2a21-f1e9-41f7-8135-8ae8006aa0c4
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=none
IPADDR=10.42.235.128
NETMASK=255.255.252.0
GATEWAY=10.42.232.1
```

i. Change ONBOOT=yes to ONBOOT=no

ii. Change BOOTPROTO=none to BOOTPROTO=dhcp

iii. Delete IPADDR, NETMASK, and GATEWAY lines.

iv. Save and exit the file.

Example

```
nas29342936_02 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
HWADDR=AC:16:2D:70:3E:BD
TYPE=Ethernet
UUID=667e2a21-f1e9-41f7-8135-8ae8006aa0c4
ONBOOT=no
NM_CONTROLLED=yes
BOOTPROTO=dhcp
```

8. Reboot the recently added node to complete configuration of the node:

```
nas> cluster reboot <node_name>
```

Note: Answer **y** if dedup message is shown:

```
Get dedup jobs status on nas550203_01 failed. Reboot/Shutdown may f →
ail dedup running jobs on nas550203_01.

Do you want to continue (y/n) y
```

This extra reboot is required, even though the node rebooted at the end of the add operation.

9. Check that both nodes are running (this can take 5-10 minutes):

```
> cluster show
Node State CPU(15 min) bond0(15 min)
 % rx(MB/s) tx(MB/s)
---- ----- ----------- -------- --------
node_01 RUNNING 3.42 1.50 3.72
node_02 RUNNING 13.32 11.19 18.02
```

10. Verify the VIPs are balanced by repeatedly running the `network ip addr show` command until balanced:

```
> network ip addr show
IP Netmask/Prefix Device Node Type Status
-- -------------- ------ ---- ---- ------
10.1.1.2 255.255.252.0 bond0 nas551011_01 Physical
10.1.1.3 255.255.252.0 bond0 nas551011_02 Physical
10.1.1.10 255.255.252.0 bond0 nas551011_01 Virtual ONLINE (Con IP)
10.1.1.11 255.255.252.0 bond0 nas551011_02 Virtual ONLINE
10.1.1.12 255.255.252.0 bond0 nas551011_01 Virtual ONLINE
```

11. Log out to become a support user.

12. Check that the Access NAS Configuration Kit files still exist on the node:

```
# ls /media/config
```

13. If the files still exist, then skip to Step 16 to configure the cluster:

    If necessary, create a directory to store the Access NAS Configuration Kit.

```
# mkdir -p /media/config
```

14. Download and copy the Access NAS Configuration Kit into the directory created in previous step. Check relevant deployment release note for revision information.

15. Install the Access NAS Configuration Kit by entering the following commands where `<ver>` represents the version of the Access NAS Configuration Kit, and `<version>` represents the version of the extracted RPM.

```
# cd /media/config
# tar xvf 19089-CXP9033343_X_<ver>_TAR_GZIPV1.tar.gz
# yum install ERICnasconfig_CXP9033343-<version>.rpm -y
```

16. Configure the cluster using the following commands and answer yes to all the questions.

```
# cd /media/config
# ./configure_NAS.bsh -a rpm
```

Note: Reboot may occur.

17. If a reboot did not occur in Step 16 then reboot the recently added node to complete configuration of the node:

```
nas> cluster reboot <node_name>
```

18. Verify the reboot has started:

```
# su - master
> cluster show
Node State CPU(15 min) bond0(15 min)
 % rx(MB/s) tx(MB/s)
---- ----- ----------- -------- --------
node_01 EXITED
node_02 RUNNING 13.32 11.19 18.02
```

19. Verify the node has rejoined to the cluster (this can take 5-10 minutes):

```
> cluster show
Node State CPU(15 min) bond0(15 min)
 % rx(MB/s) tx(MB/s)
---- ----- ----------- -------- --------
node_01 RUNNING 3.42 1.50 3.72
node_02 RUNNING 13.32 11.19 18.02
```

20. Verify the VIPs are balanced by repeatedly running the following command until balanced:

```
> network ip addr show
IP Netmask/Prefix Device Node Type Status
-- -------------- ------ ---- ---- ------
10.1.1.2 255.255.252.0 bond0 nas551011_01 Physical
10.1.1.3 255.255.252.0 bond0 nas551011_02 Physical
10.1.1.10 255.255.252.0 bond0 nas551011_01 Virtual ONLINE (Con IP)
10.1.1.11 255.255.252.0 bond0 nas551011_02 Virtual ONLINE
10.1.1.12 255.255.252.0 bond0 nas551011_01 Virtual ONLINE
```

Note: The node is added to the VA cluster.

21. Post NAS reboot, update the `CLIENT_NAME` field of the `bp.conf` file with it's respective physical hostname.

    a. Log on to the ENM MS as the brsadm user:

    ```
    # ssh -X -l brsadm <ms_ip_address>
    ```

    b. Get the list of nodes connected to MS:

    ```
    # /opt/ericsson/itpf/bur/bin/bos --operation list_nodes
    ```

Example:

```
[brsadm@ieatlmsxxx-1 root]$ /opt/ericsson/itpf/bur/bin/bos --operat →
ion list_nodes

Node: db-1 Hostname: ieatrcxb2447 IP address: 10.247.246.5 Backup I →
P: 10.151.24.72 Backup hostname:ieatrcxb2447-bkp1

Node: db-2 Hostname: ieatrcxb3031 IP address: 10.247.246.8 Backup I →
P: 10.151.24.75 Backup hostname: ieatrcxb3031-bkp1

Node: svc-1 Hostname: ieatrcxb3049 IP address: 10.247.246.24 Backup →
 IP: 10.151.24.73 Backup hostname: ieatrcxb3049-bkp1

Node: svc-2 Hostname: ieatrcxb3050 IP address: 10.247.246.25 Backup →
 IP: 10.151.24.74 Backup hostname: ieatrcxb3050-bkp1

Node: svc-3 Hostname: ieatrcxb2563 IP address: 10.247.246.3 Backup  →
IP: 10.151.24.70 Backup hostname: ieatrcxb2563-bkp1

Node: svc-4 Hostname: ieatrcxb2564 IP address: 10.247.246.4 Backup  →
IP: 10.151.24.71 Backup hostname: ieatrcxb2564-bkp1

Node: nas VIP IP address: 10.140.59.110 Hostname: ieatsfsx422-423mg →
t NAS Type: VA

Node: nas atsfsx422423_01 IP address: 10.140.59.106 Hostname: ieats →
fsx422-ph1

Node: nas atsfsx422423_02 IP address: 10.140.59.107 Hostname: ieats →
fsx423-ph1

Node: ms Hostname: ieatlmsxxx-1 IP address: 10.247.246.2 Backup IP: →
10.151.24.149 Backup hostname: ieatlmsxxx-1-bkp1
```

c. Take note of the respective NAS physical hostnames from this list.

d. Log on to each NAS client and update the `CLIENT_NAME` field of the `/usr/openv/netbackup/bp.conf` file with it's respective physical hostname.

5.13.10.5 Assign IP Address to Heartbeat Interface when Adding a Node to the Cluster

This procedure describes how to assign an IP address to a heartbeat interface of a node.

This procedure should only be performed by a support engineer as part of a SFS to VA migration or a full NAS restore.

Prerequisites

— `Root` user access to the VA nodes.

— RHEL and relevant patches are installed on the node.

— Heartbeat interfaces have been identified using the NIC Identification Procedure.

— Installation interface used to install VA node is known.

Steps

1. As `root` user, log on to the iLO console of the node to be added to the cluster.
2. Run the NIC identification script as follows:

   ```
   # /opt/ericsson/NASconfig/bin/ident_nics.sh <installation NIC>
   ```

   where `<installation NIC>` is the name of the installation interface used to install the VA node.
3. Determine the name of the first heartbeat interface by examining the Purpose column in the output of the above script.

   In the example below the first heartbeat interface is eth4.

   Example

   ```
   11:28:56   [INFO]
   Checking NICs on local_node. This will take a few moments..

   NIC Information for nas_01
   ------------------------------------------------------------------------
    Interface |  Bus ID |  Driver |    Purpose | Comment
   ------------------------------------------------------------------------
          eth0 | 07:00.0 |   bnx2x |       bond | -
          eth1 | 07:00.1 |   bnx2x |       bond | -
          eth2 | 24:00.0 |   bnx2x |       bond | -
          eth3 | 24:00.1 |   bnx2x |       bond | -
         eth10 | 27:00.2 |     igb |    exclude | -
          eth5 | 03:00.1 |     tg3 |    exclude | -
          eth6 | 03:00.2 |     tg3 |    exclude | -
          eth7 | 03:00.3 |     tg3 |    exclude | -
          eth8 | 27:00.0 |     igb |    exclude | -
          eth9 | 27:00.1 |     igb |    exclude | -
          eth4 | 03:00.0 |     tg3 |  heartbeat | -
         eth11 | 27:00.3 |     igb |  heartbeat | -
   ```
4. Configure the IP address in the network configuration file for the heartbeat interface. In the following example, `eth<XX>` represents the NIC of the first heartbeat interface.

   ```
   # vim /etc/sysconfig/network-scripts/ifcfg-eth<XX>
   ```

   Make the following additions and changes to the file.

   a. Change `ONBOOT=no` to `ONBOOT=yes`

   b. Change `BOOTPROTO=dhcp` to `BOOTPROTO=none`

   c. Add the line `IPADDR=172.16.0.99`

   d. Add the line `NETMASK=255.255.255.0`

   e. Add the line `GATEWAY=172.16.0.1`

   f. Save and exit the file.

5. Bring up the heartbeat interface. In the following example, `eth<XX>` represents the first heartbeat interface.

```
# ip link set eth<XX> up
```

6. Restart the network service as follows:

```
# service network restart
```

7. Verify that the IP address is assigned to the heartbeat interface. In the following example, `eth<XX>` represents the first heartbeat interface.

```
# ip addr show dev eth<XX>
```

Example

```
# ip addr show dev eth4
eth4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    link/ether 32:63:ba:45:c1:39 brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.99/24 brd 172.16.0.255 scope global eth4
    inet6 fe80::3a63:bbff:fe45:a139/64 scope link
       valid_lft forever preferred_lft forever
```

Results

An IP address is assigned to a heartbeat interface on the node.

5.13.10.6 Emergency Access to the VA Node

> This topic describes the steps to access a Veritas Access node when the normal Storage VLAN pathway is not functioning.

Configure a Temporary Interface

Access to a VA node can be useful in certain conditions, for example when configuring bonding or VLAN tagging, when access through the normal Storage VLAN is not possible and access through the iLO is not sufficient. For example, the iLO might be busy executing a script, or there is a need to transfer software to the node, which is not possible through the iLO.

The provided script creates a network interface configuration file and connect the interface. It will also modify the firewall (iptables) configuration, so access is allowed over the new interface. If the node is restarted for any reason, the firewall configuration is reset and access is denied.

It's recommended to configure the interface once (temporary), so valid values can be saved. When access is really needed, no values need to be provided.

The script has to be executed on each node where access to the interface is required.

This procedure is availble for both ENM VA and classic (ENIQ) VA.

Note: This is an optional procedure and is not recommended as a permanent configuration. When done, the confguration should be removed.

Note: This procedure must not be applied if the node has already been setup with a connection to the ENM central email relay via the same interface.

5.13.10.6.1 Configure NAS Install NIC

The topic describes the tasks required to configure a temporary network interface on the internal VLAN.

This is an optional task and is applicable for both nodes in the Veritas Access deployment. It is performed using `support` user after installation of the VA NAS cluster.

Note: This procedure must not be applied if the node has already been setup with a connection to the ENM central email relay via the same interface.

Prerequisites

- NAS is installed and configured with Access NAS Configuration Kit.
- Login credentials to the Veritas Access NAS as `support` user are known.
- Login credentials to the iLO are known.
- The network interface (NIC) to configure is known. Normally the same 1Gb interface that was used when installing the VA NAS.
- The interface must be cabled as per the *Network and Storage Cabling* section of the page 354 or per the *EMC VNX Configuration* for OSS-RC and ENIQ for classic systems.
- IP address and netmask to configure must be known. Optionally a gateway for that interface.

Configuration values have to be provided the first time the script is executed. In the subsequent operations they can be omitted. If new values are required, apply Step 1 again.

Steps

1. Configure the interface:

```
# /opt/ericsson/NASconfig/bin/plumb_install_nic.sh -a plumb -n <nic> -i <ip> →
 -m <netmask> [-g <gateway>]
```

   It is optional to configure a gateway/router on this interface.

The values used are stored in a file for re-use next time: `/opt/ericsson/NASconfig/etc/install_nic`

2. When emergency access is no longer required, disconnect the interface:

```
# /opt/ericsson/NASconfig/bin/plumb_install_nic.sh -a unplumb [-n <nic>]
```

The interface should be disconnected. It is not recommended to retain the interface on a permanent basis. The interface can be specified, but if not, the value will be taken from the saved file.

3. To configure the interface when initial setup has been done:

```
# /opt/ericsson/NASconfig/bin/plumb_install_nic.sh -a plumb
```

If the script has been launched initially, parameters can be omitted. If different values are needed, just provide new values.

4. When emergency access is no longer required, disconnect the interface:

```
# /opt/ericsson/NASconfig/bin/plumb_install_nic.sh -a unplumb
```

Results

Access to the VA node via the installation interface.

5.13.11 Reinstall One or Both Nodes in the Cluster

If you need to reinstall one node in the cluster, follow the section Remove and Re-Add a Node on page 99, for the node to be re-added.

If you need to reinstall both nodes in the cluster, follow the section Remove and Re-Add a Node on page 99 below for one node, then repeat for the other node.

5.13.11.1 Identify Prerequisite Information

Context Description

Media and information required for the procedure identified.

Steps

For Unity, do the following:

— Identify Prerequisite Information on Unity on page 97

For VNX, do the following:

— Identify Prerequisite Information on VNX on page 98

Results

Prerequisite information recorded and required media identified.

5.13.11.1.1 Identify Prerequisite Information on Unity

Prerequisites

For ENM, Deployment SED with Veritas Access details is available.

Steps

1. Log on to the MS as root user, then run the following command to determine the ID of the NAS host and the IDs of the accessible LUNs:

   ```
   # uemcli -d <sp_ip> /remote/host show -filter "ID,Name,Accessible LUNs"
   ```

   Where:

   Table 5

Parameter	Explanation
`<sp_ip>`	IP address of the Unity array.

   Record the Host ID and all the LUNs attached to the NAS host for later use.

2. Record the temporary Installation IP to be used later in the Install RHEL OS section.

3. Check the media requirements.

   Make sure that you have access to the following media, which is required to perform an initial installation:

   Table 6 Veritas Access Initial Install Media

Media	Product No.
RHEL 7.6 Media	19089-CXP 903 7123
Access NAS RHEL OS Patch Set	19089-CXP 903 6738
Access NAS Configuration Kit	19089-CXP 903 3343

   For information about the revisions of the required software, refer to the *ENM Release Note* of the pertinent product.

Results

Prerequisite information on Unity SAN recorded and required media identified.

5.13.11.1.2 Identify Prerequisite Information on VNX

Prerequisites

For ENM, Deployment SED with Veritas Access details is available.

Steps

1. Log on to the NAS management console IP address as user master and run the following command for the node, to get the WWN which are online:

```
nas> storage hba <hostname>
```

Example output:

```
nas> storage hba nas_01
HBA_Node_Name            WWN                      State    Speed Support_Classes Transmitted_FC_Fr →
ames Received_FC_frames  Link_Failure_Count
-------------            ---                      -----    ----- --------------- -----------------  →
---- ------------------  ------------------
50:01:43:80:33:14:3b:89  50:01:43:80:33:14:3b:88  online   8_Gbit  Class_3         2974392834       →
        2740769863               1
50:01:43:80:33:14:3b:8b  50:01:43:80:33:14:3b:8a  online   8_Gbit  Class_3         240604717        →
        1851278771               1
```

2. Log on to the MS as root user, then run the following command to get details of the storage groups:

```
# /opt/Navisphere/bin/naviseccli -h <spa> -user <username> -password <password> -scope 0 storagegr →
oup -list
```

Where:

Table 7

Parameter	Explanation
<spa>	The storage processor A IP address.
<username>	The admin username for the SAN.
<password>	The admin password for the SAN.

Determine the Storage Group name for the NAS node by matching the HBA UID with the HBA value from the first step.

3. From the MS run the following command to get details of hosts connected to the NAS storage group:

```
# /opt/Navisphere/bin/naviseccli -h <spa> -user <username> -password <password> -scope 0 storagegr →
oup -list -gname <SGName> -host
```

Where:

Parameter	Explanation
<spa>	The storage processor A IP address.
<username>	The admin username for the SAN.
<password>	The admin password for the SAN.
<SGName>	The NAS Storage Group name.

Example:

```
# /opt/Navisphere/bin/naviseccli -h 12.34.56.78 -user admin -password Password -scope 0 storagegro →
up -list -gname VA_SG -host
```

Ensure the `HBA UID` matches the HBA values determined in Step 1. Record the `Host name` corresponding to the NAS hostname for later use.

4. Record the temporary Installation IP to be used later in the Install RHEL OS section.

5. Check the media requirements.

   Make sure that you have access to the following media, which is required to perform an initial installation:

   Table 8 Veritas Access Initial Install Media

Media	Product No.
RHEL 7.6 Media	19089-CXP 903 7123
Access NAS RHEL OS Patch Set	19089-CXP 903 6738
Access NAS Configuration Kit	19089-CXP 903 3343

   For information about the revisions of the required software, refer to the *ENM Release Note* of the pertinent product.

Results

Prerequisite information on VNX SAN recorded and required media identified.

5.13.11.2 Remove and Re-Add a Node

Context Description

A node will be removed from the cluster and then re-added to the cluster.

Prerequisites

The node to be re-added has been identified.

Expected Result

Node is re-added to the cluster

5.13.11.2.1 Remove Node from Cluster

Remove the node to be re-added from the cluster.

Prerequisites

The node to be reinstalled has been identified.

Expected Result

Node is removed from the cluster.

Steps

1. Log on to management console as user master via the management console VIP.
2. Shutdown node to be reinstalled.

```
nas> cluster shutdown <name of node to be reinstalled>
```

3. Wait for node to power off.
4. If the node to be re-added was the master node, you will need to reconnect to the management console after 30 seconds and log on to the management console as user master
5. Check the state of the cluster.

```
nas> cluster show
Node         State    CPU(15 min)   bond0(15 min)
%  rx(MB/s) tx(MB/s)
----         ----     ----------    ----------
nas_01   EXITED
nas_02   RUNNING    1.47        0.00   0.00
```

The node being reinstalled will show a State of Exited.

6. Remove the node from the cluster.

```
nas> cluster del <name of node to be reinstalled>
```

```
       100% [#] Deleting <name of node to be reinstalled> con
figuration from the cluster
       Node <name of node to be reinstalled> deleted from the
 cluster
```

7. Verify that the node has been removed from the cluster.

```
nas> cluster show
Node         State    CPU(15 min)   bond0(15 min)
%  rx(MB/s) tx(MB/s)
----         ----     ----------    ----------
nas_02   RUNNING    1.47        0.00   0.00
```

8. Verify that no services on the cluster are faulted.

```
nas> support services showall
```

Note: At this point, the node to be reinstalled is only accessible through the iLO.

5.13.11.2.2 Disconnect NAS Host from SAN Storage

Before installing the operating system the node must be removed from the SAN. For Unity, the LUNs are removed from the NAS host. For VNX, the node is removed from the storage group.

Steps

For Unity, do the following:

— Remove LUNs from the NAS Host on Unity on page 102

For VNX, do the following:

— Remove Node from the Storage Group on VNX on page 103

Results

The node is removed from the SAN.

5.13.11.2.2.1 Remove LUNs from the NAS Host on Unity

Prerequisites

— The node has been removed from the cluster.

— NAS host ID and IDs of LUNs have been gathered.

Steps

1. Log on to the MS as `root` user.
2. Remove the LUNs from the NAS host. Repeat the below command until all LUNs attached to the NAS host have been removed.

```
# uemcli -d <sp_ip> /remote/host -id <host_id> set -removeLuns <lun_id>
```

Where:

Table 9

Parameter	Explanation
<sp_ip>	IP address of the Unity array.
<host_id>	The ID of the NAS host. This information was recorded in Prerequisite Information on Unity section.
<lun_id>	The ID of the LUN attached to the NAS host. This information was recorded in Prerequisite Information on Unity section.

Example

```
# uemcli -d 12.34.56.78 /remote/host -id Host_102 set -removeLuns sv_1012
```

3. Confirm that the LUNs have been removed from the NAS host. If all the LUNs have been removed from the NAS host the command should not return any output. If LUNs are listed in the output, remove them from the NAS host as described in step 2.

```
# uemcli -noHeader -d <sp_ip> /remote/host/hlu -host <host_id> show -detail
```

Where:

Table 10

Parameter	Explanation
<sp_ip>	IP address of the Unity array.
<host_id>	The ID of the NAS host. This information was recorded in Prerequisite Information on Unity section.

Example

```
# uemcli -noHeader -d 12.34.56.78 /remote/host/hlu -host Host_102 show -deta →
il
```

Results

The LUNs have been removed from the NAS host.

5.13.11.2.2.2 Remove Node from the Storage Group on VNX

Prerequisites

— The node has been removed from the cluster.

— HBA WWN information has been gathered.

Steps

1. Log on to the MS as `root` user.
2. Remove the node from the Storage Group.

```
# /opt/Navisphere/bin/naviseccli -h <spa> -user <username> -p →
assword <password> -scope 0 \
                            storagegroup -disconnecthost -hos →
t <SAN_NAS_hostname> -gname <VASGName> -o
```

Where:

Table 11

Parameter	Explanation
<spa>	The storage processor A IP address.
<username>	The admin username of the SAN.
<password>	The admin password of the SAN.
<SAN_NAS_hostname>	The host name of the NAS node on SAN. This information was recorded in Prerequisite Information section.
<VASGName>	The NAS Storage Group name.

Example

```
      # /opt/Navisphere/bin/naviseccli -h 12.34.56.78 -user a →
```

```
dmin -password Password -scope 0 \
      storagegroup -disconnecthost -host nas_hostname -gname
VA_SG -o
```

Results

The node has been removed from the Storage Group.

5.13.11.2.3 HPE Rack Server Configuration

This section describes the steps to configure Gen10, Gen9 or Gen8 HPE rack servers.

Prerequisites:

- HPE ProLiant Gen10, Gen9 or Gen8 rack servers.
- Advanced iLO Manager Licenses for the rack server iLO modules.

Steps

- Configure the iLO IP Address on page 104
- Add iLO Licenses to HPE ProLiant Rack Servers on page 105
- ENM MS Gen10 Rack Server BIOS Procedure on page 108
- ENM MS Gen9 Rack Server BIOS Procedure on page 110
- Gen8 Rack Server BIOS Procedure

Results

Rack hardware configuration has been completed successfully.

5.13.11.2.3.1 Configure the iLO IP Address

This section describes how to configure the IP address for the HPE rack server iLO.

Prerequisites

- HPE Gen10, Gen9 or Gen8 rack server.
- IP address to assign to the rack server iLO.

Steps

1. Refer to the appropriate document for information on configuring the IP address for the server iLO.
    a. Gen10. Refer to *HPE iLO User Guide* mentioned in the *Reference List*.
    b. Gen8 and Gen9. Refer to *HPE iLO User Guide* mentioned in the *Reference List*.

Results

The iLO for a rack server is assigned an IP address and is accessible.

5.13.11.2.3.2 Add iLO Licenses to HPE ProLiant Rack Servers

This section describes how to add an iLO license to HPE ProLiant Gen10, Gen9 or Gen8 rack servers.

Prerequisites

— Administrator user access to the HPE iLO interface.

— iLO Advanced License key for each rack server.

Steps

1. Log on to the iLO as `Administrator` using SSH.
2. Check the license installed on the rack server.
    a. Run the following command on Gen10 rack servers:

```
</>hpiLO-> show /map1/oemHPE_license1
```

Example

```
hpiLO-> show /map1/oemHPE_license1
status=0
status_tag=COMMAND COMPLETED
Wed Oct 3 10:10:23 2018


/map1/oemHPE_license1
Targets
Properties
oemHPE_name1=iLO Standard
oemHPE_key1=XXXXXXXXXXXXXXXXXXXXHM9BM
oemHPE_name2=None
oemHPE_key2=0
oemHPE_name3=None
oemHPE_key3=0
Verbs
cd version exit show oemHPE_licenseinstall
```

    b. Run the following command on Gen9 and Gen8 rack servers:

```
</>hpiLO-> show /map1/oemhp_license1
```

Example

```
hpiLO-> show /map1/oemhp_license1
status=0
status_tag=COMMAND COMPLETED
Tue Oct 2 15:18:36 2018


/map1/oemhp_license1
Targets
Properties
oemhp_name1=iLO 4 Standard
oemhp_key1=xxxxxxxxxxxxxxxxxxxxABCDE
oemhp_name2=None
oemhp_key2=0
oemhp_name3=None
oemhp_key3=0
Verbs
cd version exit show oemhp_licenseinstall
```

If the license name contains "Standard", proceed to *Step 3*. Do not exit the iLO CLI.

If the license name contains "Advanced" the license is already configured. Log out of the iLO and do not proceed to *Step 3*.

```
</>hpiLO-> exit
```

Repeat this procedure from *Step 1* until all rack servers are configured.

3. Install the license key.

    a. Run the following commands on Gen10 rack servers:

    ```
    </>hpiLO-> cd /map1/oemHPE_license1
    </map1/oemHPE_license1>hpiLO-> oemHPE_licenseinstall AAAAA-BBBBB-CC →
    CCC-DDDDD-EEEEE
    ```

    Where AAAAA-BBBBB-CCCCC-DDDDD-EEEEE is the iLO Advanced License key.

    b. Run the following commands on Gen9 or Gen8 rack servers:

    ```
    </>hpiLO-> cd /map1/oemhp_license1
    </map1/oemhp_license1>hpiLO-> oemhp_licenseinstall AAAAA-BBBBB-CCCC →
    C-DDDDD-EEEEE
    ```

    Where AAAAA-BBBBB-CCCCC-DDDDD-EEEEE is the iLO Advanced License key.

The following output is displayed when the license is successfully installed:

```
status=0
status_tag=COMMAND COMPLETED
New license key installed
```

4. Verify that the advanced license is installed.

    a. Run the following command on Gen10 rack servers:

    ```
    </>hpiLO-> show /map1/oemHPE_license1
    ```

    Example

    ```
    hpiLO-> show /map1/oemHPE_license1
    status=0
    status_tag=COMMAND COMPLETED
    Wed Oct 3 10:10:23 2018


    /map1/oemHPE_license1
    Targets
    Properties
    oemHPE_name1=iLO Advanced
    oemHPE_key1=XXXXXXXXXXXXXXXXXXXXHM9BM
    oemHPE_name2=None
    oemHPE_key2=0
    oemHPE_name3=None
    oemHPE_key3=0
    Verbs
    cd version exit show oemHPE_licenseinstall
    ```

    b. Run the following command on Gen9 and Gen8 rack servers:

    ```
    </>hpiLO-> show /map1/oemhp_license1
    ```

    Example

    ```
    hpiLO-> show /map1/oemhp_license1
    status=0
    status_tag=COMMAND COMPLETED
    Tue Oct 2 15:18:36 2018


    /map1/oemhp_license1
    Targets
    Properties
    oemhp_name1=iLO 4 Advanced
    oemhp_key1=xxxxxxxxxxxxxxxxxxxxABCDE
    oemhp_name2=None
    oemhp_key2=0
    oemhp_name3=None
    oemhp_key3=0
    Verbs
    cd version exit show oemhp_licenseinstall
    ```

5. Repeat this procedure from *Step 1* for any other rack server until all rack servers are configured.

Results

The license is added to the rack server iLO interface. This enables the user to mount an ISO remotely as well as use the iLO remote console.

5.13.11.2.3.3 ENM MS Gen10 Rack Server BIOS Procedure

This section provides information on how to configure the BIOS settings for Gen10 rack servers.

The procedure is applicable for the following server:

— ENM MS

Prerequisites

— A Gen10 rack-mounted server with correct hardware installed.

— Administrator access to a Gen10 rack server iLO Remote Console.

Steps

1. Open an iLO Remote Console and confirm that the rack server is ready to configure.
    a. If the rack is powered on, reset the rack. Otherwise, power on the rack.
    b. Press **F9** when prompted to access the **System Utilities** menu.
    c. From the **System Utilities** menu, select **System Configuration**.
2. The layout in the *Required BIOS Settings for ENM MS Gen10 Rack Server* display the setting name, the desired value, and the setting location in the BIOS. Follow the table layout to find and apply the required settings for the server:

Table 12 Required BIOS Settings for ENM MS Gen10 Rack Server

Setting	ENM MS	Location
Boot Mode	Legacy BIOS Mode	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options** > **Boot Mode**
Workload Profile	Virtualization - Max Performance	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Workload Profile**
Intel(R) Hyper-Threading	Enabled	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Processor Options**

Setting	ENM MS	Location
Virtual Serial Port	COM 1; IRQ 4; I/O: 3F8h-3FFh	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Serial Port Options**
PCIe Device Disable	Auto(1)	All devices in **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **PCIe Device Configuration**
PCIe Link Speed	Auto(1)	
PCIe Option ROM	Enabled(1)	
Date (mm.dd.yyyy)	Set date(2)	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Date and Time**
Time (hh mm ss)	Set time(2)	
Time Zone	See note(2)(3)	
Daylight Savings Time	See note(2)	
Time Format	Coordinated Universal Time (UTC)	
Embedded LOM Port 1	Disabled	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options**
Embedded FlexibleLOM 1 Port 1	N/A	
Embedded FlexibleLOM 1 Port 2	N/A	

(1) The PCIe Device Configuration setting should be applied to any of the following:

- Embedded Storage 1 OR Embedded RAID 1 : HPE SmartArray P408i-a SR Gen10
- Embedded LOM 1 : HPE Ethernet 1GB 4-port 331i Adapter - NIC
- Embedded FlexibleLOM : HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter - NIC
- Slot x : HPE Ethernet 10Gb 2- port 562SFP+Adapter - NIC
- Slot x : HPE SN1200E 16Gb 2p FC HBA - FC1

(2) This setting is specified at the discretion of the customer.

(3) Only a subset of global time zones are available. Select the UTC offset for your location.

Note:
- Apply the setting to all devices.
- If the ENM Management (iLO Access) network is non-routed, the 1Gb interfaces are used. To configure the Management interface on the ENM Management (Server Access) network, refer to *Configure the Management Interface on the Management Server*.

3. Exit the BIOS, saving the configuration and rebooting the server.
4. Close the iLO Remote Console and return to the rack iLO web interface.
5. Set the iLO time zone.

a. Navigate to the **iLO Dedicated Network Port** > **SNTP** page.

b. Ensure that **Use DHCPv4 Supplied Time Settings** is unchecked.

c. Select the location and time zone for the server in the **Time Zone** dropdown menu.

Note: Only a subset of global time zones are available. Select the UTC offset for your location.

d. Click **Apply**.

6. Set the iLO server name.

a. Navigate to the **Security** > **Access Settings** page.

b. In the **Server** section, enter the server name in the **Server Name** text field.

c. Click **OK**.

7. Configure IPMI/DCMI over LAN.

a. Navigate to the **Security** > **Access Settings** page.

b. In the **Network** section, ensure that **IPMI/DCMI over LAN** is checked.

c. In the **Network** section, ensure that **IPMI/DCMI over LAN Port** is set to **623**.

d. Click **OK**.

e. Click **Yes, apply and reset**.

Note: When the iLO is reset, it can take several minutes to re-establish a connection.

Results

The rack server required BIOS parameters have been set.

5.13.11.2.3.4 ENM MS Gen9 Rack Server BIOS Procedure

This section provides information on how to configure the BIOS settings for Gen9 rack servers.

The procedure is applicable for the following servers:

— ENM MS

Prerequisites

— A Gen9 rack-mounted server with correct hardware installed.

— Administrator access to a Gen9 rack server iLO Remote Console.

Steps

1. Open an iLO Remote Console and confirm that the rack server is ready to configure.
    a. If the rack is powered on, reset the rack. Else, power on the rack.
    b. Press **F9** when prompted to access the **System Utilities** menu.
    c. From the **System Utilities** menu, select **System Configuration**.
2. The layout in the table *Required BIOS Settings for ENM MS Gen9 Rack Server Types* display the setting name, the desired value, and the setting location in the BIOS. Follow the table layout to find and apply the required settings for each server type:

Table 13 Required BIOS Settings for ENM MS Gen9 Rack Server Types

Setting	ENM MS	Location
Boot Mode	Legacy BIOS Mode	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Boot Options**
Power Profile	Maximum Performance	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Power Management**
Embedded RAID OR Embedded RAID: Smart Array P440ar Controller (1)	Enabled	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **PCI Device Enable/ Disable**
Embedded LOM 1 OR Embedded LOM 1 : HP Ethernet 1Gb 4-port 331i Adapter - NIC	Enabled(2)	
HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter - NIC	Enabled	
Embedded SATA Controller: Intel SATA Controller	Enabled	
Slot x : HP Ethernet 10Gb 2-port 560SFP+ Adapter - NIC (1)	Enabled	
Date (mm-dd-yyyy)	Set Date(3)	**System Configuration** > **BIOS/Platform**
Time (hh:mm:ss)	Set Time (3)	

Setting	ENM MS	Location
Daylight Saving Time	See note(4)	**Configuration (RBSU)** > **Date and Time**
Time Format	Coordinated Universal Time (UTC)	
Embedded LOM Port 1	Disabled	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Network Options** > **Network Boot Options**
Embedded FlexibleLOM 1 Port 1	N/A	
Embedded FlexibleLOM 1 Port 2	N/A	
Intel (R) Hyperthreading	Enabled	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Processor Options**
Virtualization Technology	Enabled	**System Configuration** > **BIOS/Platform Configuration (RBSU)** > **System Options** > **Virtualization Options**
Intel(R) VT-d	Enabled	
SR-IOV	Enabled	

(1) Apply the setting to all items containing the same name.

(2) If the ENM Management (iLO Access) network is non-routed, the 1Gb interfaces must be enabled. To configure the Management interface on the ENM Management (Server Access) network, see section *Configure the Management Interface on the Management Server* in the *ENM Installation Instructions* document. If the ENM Management (iLO Access) network is routed, then set the option to `Disabled`.

(3) Query the time from the site NTP server. If a site NTP server is not available, obtain the most accurate time source available.

(4) This setting is specified at the discretion of the customer.

3. Configure IPMI/DCMI over LAN.

    a. If the iLO log in session has timed out, log on to the rack server iLO web interface.

    b. Navigate to the **Administration** > **Access Settings page**.

    c. In the **Service** section, set the **IPMI/DCMI over LAN Access** field to **Enabled**.

    d. In the **Service** section, set the **IPMI/DCMI over LAN Port** to **623**.

    e. Click **Apply**.

    f. Click **OK** to apply the new settings and reset the iLO.

    Note: When the iLO is reset, it can take several minutes to re-establish a connection.

Results

The rack server required BIOS parameters have been set.

5.13.11.2.3.5 Gen10 or Gen9 Create a Logical Volume

To deploy software on the Gen10 or Gen9 rack servers, a logical volume is created on the physical drives.

This procedure is applicable for the following servers:

— ENM MS: Gen10 and Gen9

— Streaming Cluster rack servers: Gen10 and Gen9

— Fallback Cluster rack servers: Gen10 and Gen9

Prerequisites

— The relevant Rack Server BIOS Procedure has been completed:

- ENM MS Gen10 Rack Server BIOS Procedure on page 108
- ENM MS Gen9 Rack Server BIOS Procedure on page 110

Steps

1. Open an **iLO Remote Console** and navigate to **Intelligent Provisioning**.
    a. Log in to the rack server iLO web interface and open an iLO Remote Console.
    b. If the server is powered on, reset the server. Otherwise, power on the server.
    c. Press **F10** when prompted to enter **Intelligent Provisioning**.
2. Select **HP Smart Storage Administrator** or **Smart Storage Administrator** before the countdown ends.

    Note: If no selection is made in this menu within 15 seconds, the default option **HP Intelligent Provisioning** or **Intelligent Provisioning** is selected automatically.
3. The **Smart Storage Administrator** quick navigation menu is at the top of the screen. Click the down arrow and select **HPE Smart Array <Model> in <Slot>** or **Smart Array <Model> in <Slot>**.
4. Under **Actions**, select **Configure**.
5. Determine the RAID level for the new array from the following table:

Table 14 Disk Count and Raid Level

Server Type	Disk Count	RAID Level
ENM MS	4	RAID 1+0
NAS	4	RAID 1+0
	2	RAID 1
Streaming Cluster rack server	4	RAID 1+0
	2	RAID 1

6. Click **Create Array**.

    a. Select all physical drives.

    b. Click **Create Array**, acknowledging any confirmation messages.

    c. Select the appropriate **RAID Level** from the 'Disk Count and Raid Level' table. Use default selections for the **Strip Size** / **Full Stripe Size**, **Sectors/ Track**, **Size** and **Caching** settings.

    d. Click **Create logical drive**.

    e. Select **Finish**.

7. In the **Configure** panel, under **Controller Devices > Logical Devices**, verify that there is 1 array with 1 logical drive.

8. For the Streaming Cluster rack servers, under the **Smart Storage Administrator** menu, select the device **HP Smart Array P440ar** > **Configure**.

    Select **Logical Devices** in the first column. In the second column, select **Logical Drive 1**.

    The Drive Unique ID for the logical volume is displayed in the third column. Scroll to the bottom of the third column and take note of the Drive Unique ID for inclusion in the ENM SED.

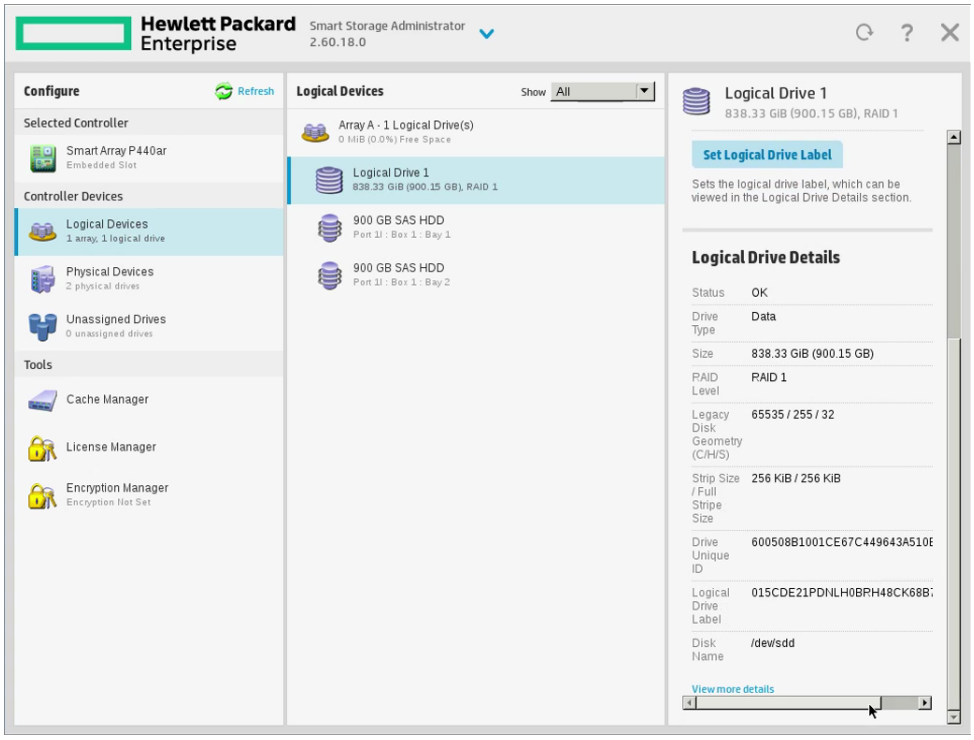


Figure 4 Identifying Streaming Cluster Rack Server Logical Drive UUID example

9. In the upper right corner, select **X** to exit the **Smart Storage Administrator**.
10. Confirm the exit and reboot the system.

Results

A logical volume has been created.

5.13.11.2.3.6 Gen8 Rack Server BIOS Procedure

This section provides information on how to configure the BIOS settings for Gen8 rack servers.

The instructions for this section are applicable for the following servers:

— ENM MS

— NAS Cluster

Prerequisites

— The HPE iLO Advanced license is applied for the rack server iLO Manager.

Steps

1. Open an iLO Remote Console and confirm that the rack server is ready to configure.

    a. Log on to the rack server iLO web interface and open an iLO Remote Console.

    b. Select **Power Switch** > **Reset** to reset the server. If the server is powered off, select **Power Switch** > **Momentary Press**.

    c. From the iLO Remote Console, press **F9** when prompted to enter the **Setup** menu.

2. The layout in table: *Required BIOS setting for Gen8 Rack Server Types* displays the setting name, the desired value, and the setting location in the BIOS. Follow the table layout to find and apply the required settings for each server type:

Table 15 Required BIOS settings for Gen8 Rack Server Types

Setting	ENM MS	NAS Cluster	Location
Embedded SATA Configuration	Enable SATA AHCI Support		**Setup** > **System Options** > **SATA Controller Options**
HP Power Profile	Maximum Performance		**Setup** > **Power Management Options**
Embedded RAID OR Smart Array P420i Controller [1]	Enabled		**Setup** > **PCI Device Enable/Disable**
HP Ethernet 10Gb 2-port 530SFP+ Adapter [1]	Enabled		
Flexible NIC OR FlexibleLOM 1 HP Ethernet 1Gb 4-port 331FLR 4-port Adapter [1]	Enabled [2]	Enabled	
HP NC365T PCIe Quad Port 1Gb Server Adapter	N/A	Enabled	
HP StorageWorks 82Q 8Gb PCI-e Dual Port FC HBA [1]	N/A	Enabled	
Date (mm-dd-yyyy)	Set Date		**Setup** > **Date and Time**
Time (hh:mm:ss)	Set Time [3][4]		
Intel (R) Virtualization Technology	Enabled		**Setup** > **System Options** > **Processor Options**
Intel (R) Hyperthreading Options	Enabled		**Setup** > **System Options** > **Processor Options**
Intel (R) VT-d	Enabled		**Setup** > **System Options** > **Processor Options**

Note: [1] Apply the value to all items matching the setting name.

[2] If the ENM Management (iLO Access) network is non-routed, the 1Gb interfaces must be enabled. To configure the Management interface on the ENM Management (Server Access) network, refer to *Configure the Management Interface on the Management Server*. If the ENM Management (iLO Access) network is routed, then set the option to Disabled.

[3] Query the time from the site NTP server. If a site NTP server is not available, obtain the most accurate time source available.

[4] Set the time to the current time at UTC+0.

3. Configure IPMI/DCMI over LAN.

   Note: This step is not required for the NAS Cluster.

   a. If the iLO log in session has timed out, log on to the rack server iLO web interface.

   b. Navigate to the **Administration** > **Access Settings** page.

   c. In the **Service** section, set the **IPMI/DCMI over LAN Access** field to **Enabled**.

   d. In the **Service** section, set the **IPMI/DCMI over LAN Port** field to **623**.

   e. Click **Apply**.

   f. Click **OK** to apply the new settings and reset the iLO.

      Note: When the iLO is reset, it can take several minutes to re-establish a connection.

Results

The following items are configured for Gen8 rack servers:

— Power Management set to high performance.

— Network Interfaces configured.

— DVD Drive is configured.

— Date and time are set.

— Disk volume is configured.

— Virtualization settings are configured.

— IPMI/DCMI over LAN is enabled and configured (not required for NAS Cluster).

5.13.11.2.3.7 Enable the Host Adapter Drivers for NAS Cluster

In order to use the HBA devices on a server, the Host Adapters need to be enabled. The following instructions specify how to enable the drivers for the HBA Host Adapters.

Prerequisites

— A Gen8 rack mounted server with correct hardware installed.

— Administrator access to a Gen8 rack server iLO Remote Console.

— Gen8 Rack Server BIOS Procedure completed successfully

Steps

1. Open an iLO Remote Console and confirm the rack server is ready to configure.
    a. Log on to the rack server iLO web interface and open an iLO Remote Console.
    b. Select **Power Switch** > **Reset** to reset the server. If the server is powered off, select **Power Switch** > **Momentary Press**.
2. During the boot, press **Ctrl-Q** when prompted to enter **QLogic Fast!UTIL**.
3. A menu similar to the following figure is displayed on screen

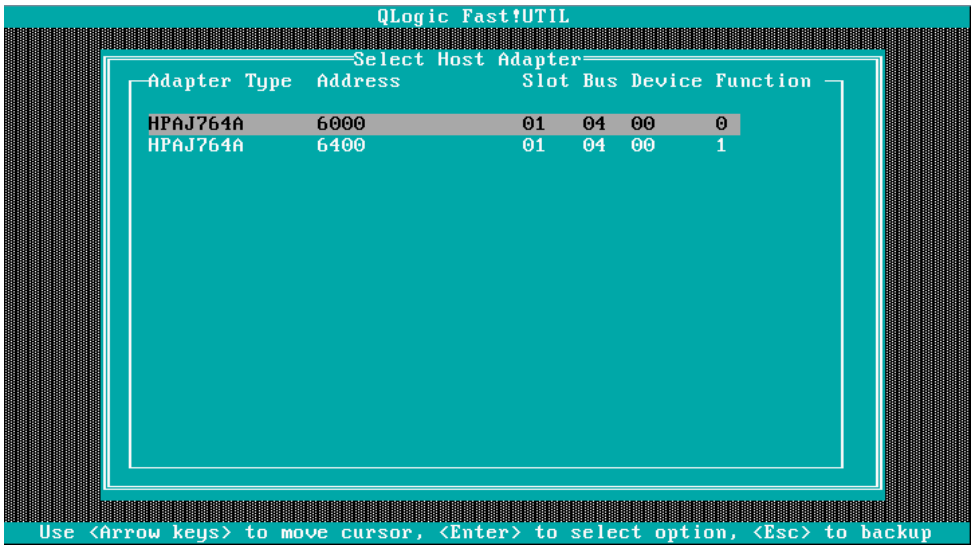


Figure 5 QLogic HBA Selection

4. Select the first Host Adapter by pressing **Enter** and select **Configuration Settings** > **Adapter Settings**. Set the **Host Adapter BIOS** setting to **Enabled** as shown in the following figure

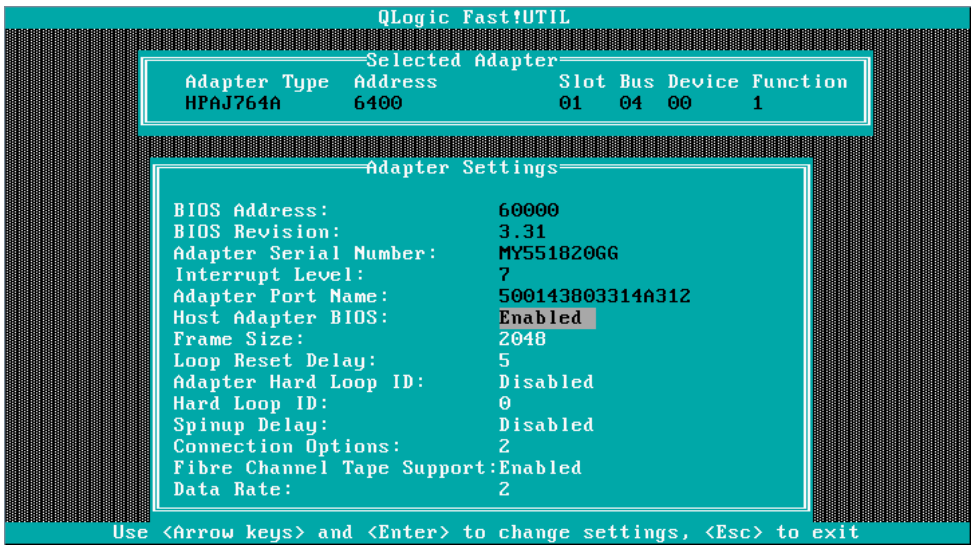


Figure 6 QLogic HBA Adapter Setting

5. Repeat Steps 3 and 4 for the second Host Adapter.

Results

The drivers for the Host Adapters are enabled successfully.

5.13.11.2.3.8 Gen8 Create a Logical Volume

In order to deploy software on the Gen8 rack servers, a logical volume is created on the physical hard drives.

Prerequisites

— Section Gen8 Rack Server BIOS Procedure is complete.

Steps

1. Log in to the rack server iLO web interface and open an iLO Remote Console.
2. Select **Power Switch** > **Reset** to reset the server. If the server is powered off, select **Power Switch** > **Momentary Press**.
3. While the server is booting, press **F8** when prompted to access the **Option ROM Configuration for Arrays Utility**.
4. Determine which RAID configuration is required.

Table 16 RAID Configuration Layout for Gen8 Rack Servers

Server Type	Disk Count	RAID Type
MS	4	RAID 1+0
NAS	4	RAID 1+0

5. Create the logical volume using the RAID type in Step 4. The following example is a logical drive RAID 1+0 on a four disk Gen8 rack server. Use default selections for the **Spare** and **Maximum Boot** partition settings.

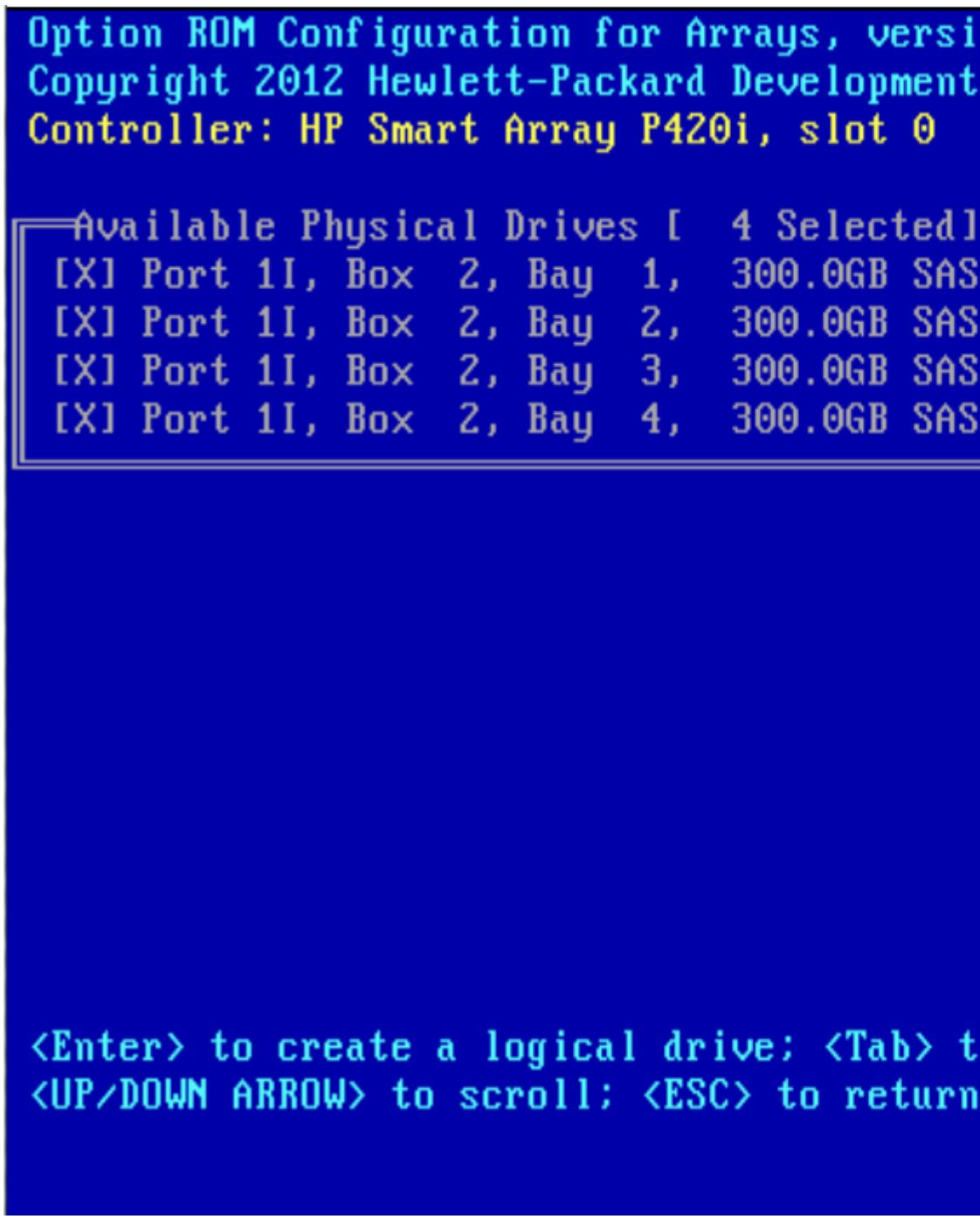


Figure 7 Option ROM Configuration for Arrays Menu

6. Press **Esc** to return to the **Option ROM Configuration** menu.
7. Save the changes made and reboot the server by returning to the **Option ROM Configuration** menu and then pressing **Esc**, **F10** then **Enter**.

Results

The logical volume has been created successfully.

5.13.11.2.4 Install RHEL OS

This section describes how to install Red Hat Enterprise Linux (RHEL), the operating system (OS) on which Veritas Access runs.

For an Initial Installation this task is applicable for both nodes in the Veritas Access deployment and you can run the task on both nodes at the same time.

Prerequisites

— OS Install media which is either on a physical DVD or as an ISO image file.

— Installation IP addresses are in place.

— Networking details (including the identity of the 1Gb NIC to be assigned an installation IP address) for each cluster node.

— Node firmware is at the level specified in FLARE and Firmware Handling Guide for HP/EMC.

— Administrator user access to the HPE iLO interface.

Steps

1. Log on to the iLO remote console.
2. Insert the RHEL ISO DVD in the DVD drive on the server or using the iLO remote console, mount the ISO by using the **Virtual Drives** > **Image File CD/DVD ROM** menu option.
3. Power on or reboot the server, as appropriate.
4. Set the one-time boot option.

   Complete the appropriate steps depending on the hardware type

   HPE ProLiant Gen9/Gen10

   a. While the server is booting, it displays **F11 Boot Menu**. Press **F11** to enter **One-Time Boot Menu**.

   b. At the **Boot Menu** screen, select the **Legacy BIOS One-Time Boot Menu** option and press **Enter**.

   c. When the **One-Time Boot Menu** is displayed, select **1** for the **One Time Boot to CD-ROM** option and press **Enter**.

   HPE ProLiant Gen8

a. While the server is booting, it displays **F11 Boot Menu**. Press **F11** to enter **One-Time Boot Menu**.

b. When the **one-time boot menu** is displayed, select **1** for the **One Time Boot to CD-ROM** option.

5. At the boot prompt, select the **Install Red Hat Enterprise Linux** option and press **Enter**.

6. The installer displays a language selection screen. Select **English** and click **Continue**

   Note: Veritas Access supports English only.

7. Select **English language** for the Language Support and the Keyboard language.

8. Click **INSTALLATION DESTINATION**, select the **HP LOGICAL VOLUME** icon. Select **I will configure partitioning** option. Click on **Done**.

   Note: If re-installing on previously installed server, ignore the warning message "Not enough free space on selected disks".

   If an existing OS related mount point exists, select the mount and delete it.

9. Create the mount points for the installation, click the text "**Click here to create them automatically**".

10. Remove `/home(rhel-home)` filesystem from the layout. Select the filesystem and click "**-**" button, if prompted to confirm delete, click on **Delete it**.

11. Modify the size of `/(rhel-root)` filesystem to use up all the available space. Select the filesystem and in the **Desired Capacity** field, enter "Max" for the logical volume and then click **Done**.

12. Click **Accept Changes** to commit changes to the filesystem layout.

13. Click **Software Selection**, select **Minimal Install**, next select **Compatibility Libraries** in the Add-Ons section. Click on **Done**

14. Click **NETWORK & HOSTNAME**. Enter the hostname (this value changes during the installation of Veritas Access). Click on **Done**.

15. Click **Date & Time**, choose your system location from the provided map, and then click **Done** to apply configuration

16. Click **Begin installation**.

17. Click **Root Password**. Enter the root password into the **Root Password** field. Type the same password into the **Confirm** field. Click on **Done**.

18. When the installation is finished, restart your system for post-installation tasks. Click **Reboot** to continue, if necessary remove the install media from the **Virtual Drives** menu

19. When the reboot is complete, log on as the root user, using the password configured in Step 17.

20. Prepare an installation IP address for each cluster node.

    This IP address is used by the Veritas Access installer, so it must not be in the physical or virtual IP pool that is used for the Veritas Access cluster later.

    Note: The temporary IP addresses are not available after the configuration of Veritas Access because they are replaced with the physical IP addresses provided at the configuration level.

21. Identify the correct interface to configure.

    a. Log on to the iLO as `Administrator` using SSH.

    b. Run the following command

    ```
    </>hpiLO-> show /system1/network1/integrated_NICs
    ```

    Example

    ```
    hpiLO-> show /system1/network1/integrated_NICs
    status=0
    status_tag=COMMAND COMPLETED
    Wed Oct 17 08:03:19 2018

    /system1/network1/integrated_NICs
    Targets
    Properties
    iLO4_MACAddress=50:65:f3:66:bc:16
    Port1NIC_MACAddress=28:80:23:a6:8a:54
    Port2NIC_MACAddress=28:80:23:a6:8a:55
    Port3NIC_MACAddress=28:80:23:a6:8a:56
    Port4NIC_MACAddress=28:80:23:a6:8a:57
    Verbs
    cd version exit show
    ```

    c. Identify MAC Address of installation interface.

       i. For Gen10 or a Gen9 server, note the MAC Address on port 1 of the Adapter.

       ii. For a Gen8 server, note the MAC Address on port 2 of the Adapter.

    d. Log out of the iLO CLI

    e. As the root user on the iLO remote console, run the `ip link show` command, find the MAC address noted in the previous step and note the interface name for the MAC address.

    ```
    # ip link show | more
    ```

22. Configure the newly-prepared IP address on the NIC and in the network configuration file. This step should be performed on the iLO remote console.

```
# vi /etc/sysconfig/network-scripts/ifcfg-<interface>
```

Make the following additions and changes to the file:

a. Change `ONBOOT=no` to `ONBOOT=yes`

b. Change `BOOTPROTO=dhcp` to `BOOTPROTO=none`

c. Add the `IPADDR=<ip address>` line where `<ip address>` is the temporary IP you are using to access the server.

   i. For ENM, specify an IP address on the Internal network.

   ii. For ENIQ-S 10Gb deployment, specify an IP address on the Services network.

   iii. For ENIQ-S 1Gb deployment, use the 11^{th} and 12^{th} IP addresses in the physical IP range on a storage network. For example, if the starting physical IP is 10.42.232.36, then the 11^{th} and 12^{th} are 10.42.232.46 and 10.42.232.47 as the install IPs.

d. Add the `NETMASK=<netmask ip>` line where `<netmask ip>` is the Subnet Netmask IP address.

e. Add the `GATEWAY=<gateway ip>` line where `<gateway ip>` is the Default Gateway IP address.

   i. For ENM, it is not necessary to specify the Default Gateway IP address.

   ii. For ENIQ-S 10Gb deployment, specify the Services VLAN Gateway as a Default Gateway.

   iii. For ENIQ-S 1Gb deployment, specify the Storage VLAN Gateway as a Default Gateway.

f. Save and exit the file.

g. Restart the network service as follows:

```
# systemctl restart network.service
```

h. Check that the interface can reach the gateway using the following command where `<interface>` represents the 1Gb NIC selected at the beginning of this step and `<gateway ip>` is the IP address of the default gateway.

```
# ping -I <interface> -c 4 <gateway ip>
```

i. For ENM `<gateway ip>` is the internal IP address of MS.

ii. For ENIQ-S 10Gb deployment, `<gateway ip>` is the Gateway IP address of Services VLAN.

iii. For ENIQ-S 1Gb deployment, `<gateway ip>` is the Gateway IP address of Storage VLAN.

23. Disable SELINUX by editing the following file:

```
# vi /etc/selinux/config
```

a. Change `SELINUX=enforcing` to `SELINUX=disabled`

b. Save and exit the file

Note: If performing a VA initial installation, verify nodes can communicate by pinging the newly-prepared IP of second node from first node once the installation IPs are up on both nodes.

If these check fails, check the cabling, Ethernet switch configuration, and BIOS configuration of both nodes. Do not proceed with VA install.

Results

RHEL is installed successfully.

Note: For Initial Installation, RHEL is installed on both nodes in the Veritas Access Cluster.

5.13.11.2.5 Reconnect NAS Host to SAN Storage

Add the node back into the Veritas Access SAN. For Unity, the LUNs are added to the NAS host. For VNX, the node is added to the storage group.

Steps

For Unity, do the following:

— Add LUNs to NAS Host on Unity on page 127

For VNX, do the following:

— Add Node to VA Storage Group on VNX on page 128

Results

The node is added to the Veritas Access SAN.

5.13.11.2.5.1 Add LUNs to NAS Host on Unity

Prerequisites

NAS host ID and IDs of LUNs are known.

Identify Prerequisite Information on page 96 has been completed.

Steps

1. Log on to the relevant MS as `root` user.
2. Add the LUNs to the NAS host. Repeat the below command until all the removed LUNs are added back to the NAS host.

```
# uemcli -d <sp_ip> /remote/host -id <host_id> set -addLuns <lun_id>
```

Where:

Table 17

Parameter	Explanation
<sp_ip>	IP address of the Unity array.
<host_id>	The ID of the NAS host. This information was recorded in Prerequisite Information section.
<lun_id>	The ID of the LUN attached to the NAS host. This information was recorded in Prerequisite Information section.

Example

```
# uemcli -d 12.34.56.78 /remote/host -id Host_102 set -addLuns sv_1012
```

3. Confirm that the LUNs have been added back to the NAS host. If all the LUNs have been added to the NAS host the command should list their IDs in the output. If LUNs are missing in the output, then add them back to the NAS host as described above.

```
uemcli -d <sp_ip> /remote/host/hlu -host <host_id> show -detail
```

Where:

Table 18

Parameter	Explanation
<sp_ip>	IP address of the Unity array.
<host_id>	The ID of the NAS host. This information was recorded in Prerequisite Information section.

Example

```
uemcli -d 12.34.56.78 /remote/host/hlu -host Host_102 show -detail
Storage system address: 12.34.56.78
Storage system port: 123
HTTPS connection

1:    ID            = Host_102_sv_1012_prod
      Host          = Host_102
      Host name     = NAS_host
      LUN           = sv_1012
      LUN name      = NAS_lun
      Snapshot      =
      Snapshot name =
      LUN ID        = 0
      Access        = Read/write
      LUN type      = Production
```

Results

The LUNs are added to the NAS host.

5.13.11.2.5.2 Add Node to VA Storage Group on VNX

Prerequisites

server_name for NAS node is known

Steps

1. Log on to the relevant MS as `root` user.
2. Add the node to the storage group.

```
     # /opt/Navisphere/bin/naviseccli -h <spa> -user <username> -password <p →
assword> -scope 0 \
     storagegroup -connecthost -host <SAN_NAS_hostname> -gname <VASGName> -o →
```

Where:

Table 19

Parameter	Explanation
<spa>	The storage processor A IP address.
<username>	The admin username for the SAN.
<password>	The admin password for the SAN.
<SAN_NAS_hostname>	The server name of the NAS node on SAN. This information was recorded in Prerequisite Information section.

Parameter	Explanation
<VASGName>	The NAS storage group name.

Example

```
# /opt/Navisphere/bin/naviseccli -h 12.34.56.78 -user admin -password Passwo
rd -scope 0 \
      storagegroup -connecthost -host nas_node -gname VA_SG -o
```

Results

The node is added to the Veritas Access storage group.

5.13.11.2.6 RHEL Patch Installation

This section describes how to install the RHEL OS patch set for Veritas Access.

For an Initial Installation this task is applicable for both nodes in the Veritas Access deployment and you can run the task on both nodes at the same time.

Prerequisites

- RHEL is installed successfully.
- Access NAS RHEL OS patch set media is available.
- Access NAS Configuration Kit is available.

Steps

1. Log on to the server iLO console as the `root` user, using the password configured during the RHEL installation.

   For more information, see Install RHEL OS on page 122.

2. Create a directory to store the Access NAS RHEL OS patch set.

   ```
   # mkdir -p /media/patches
   ```

3. Transfer the Access NAS RHEL OS patch set to the directory created in the previous step.

4. Create a directory to store the Access NAS Configuration Kit.

   ```
   # mkdir -p /media/config
   ```

5. Copy the Access NAS Configuration Kit into the directory created in the previous step.

6. Install the Access NAS Configuration Kit by entering the following commands where <ver> represents the version of the Access NAS Configuration Kit and <version> represents the version of the extracted RPM.

```
# cd /media/config
# tar xvf 19089-CXP9033343_X_<ver>_TAR_GZIPV1.tar.gz
# yum install ERICnasconfig_CXP9033343-<version>.rpm -y
```

7. Install the RHEL OS patch set for Veritas Access.

```
# /opt/ericsson/NASconfig/bin/patchrhel.bsh -u \
  /media/patches/19089-CXP9036738_Ux_<rev>.tar.gz
```

8. Reboot the server.

```
# reboot
```

Note: If performing a VA initial installation, Veritas Access RHEL OS patch set must be installed on all Veritas Access nodes.

5.13.11.2.7 Assign IP Address to Heartbeat Interface when Adding a Node to the Cluster

This procedure describes how to assign an IP address to a heartbeat interface of a node. This procedure should only be performed by a support engineer as part of a SFS to VA migration, the re-addition of a node, or a full NAS restore.

Prerequisites

— root user access to the VA nodes.

— RHEL and relevant patches are installed on the node.

— Heartbeat interfaces have been identified using the NIC Identification Procedure.

— Installation interface used to install VA node is known.

Steps

1. As root user, log on to the iLO console of the node to be added to the cluster.

2. Run the NIC identification script as follows:

```
# /opt/ericsson/NASconfig/bin/ident_nics.sh <installation NIC>
```

where <installation NIC> is the name of the installation interface used to install the VA node.

3. Determine the name of the first heartbeat interface by examining the Purpose column in the output of the above script.

```
11:28:56   [INFO]
Checking NICs on local_node. This will take a few moments..

NIC Information for nas_01
-------------------------------------------------------------------------
 Interface |  Bus ID |  Driver |    Purpose | Comment
-------------------------------------------------------------------------
    ens2f0 | 07:00.0 |   bnx2x |       bond | -
    ens2f1 | 07:00.1 |   bnx2x |       bond | -
    ens5f0 | 24:00.0 |   bnx2x |       bond | -
    ens5f1 | 24:00.1 |   bnx2x |       bond | -
      eno2 | 03:00.1 |     tg3 |    exclude | -
      eno3 | 03:00.2 |     tg3 |    exclude | -
      eno4 | 03:00.3 |     tg3 |    exclude | -
    ens6f0 | 27:00.0 |     igb |    exclude | -
    ens6f1 | 27:00.1 |     igb |    exclude | -
    ens6f2 | 27:00.2 |     igb |    exclude | -
      eno1 | 03:00.0 |     tg3 |  heartbeat | -
    ens6f3 | 27:00.3 |     igb |  heartbeat | -
```

4. Identify the interface which represents the first heartbeat interface, and configure the IP address in the corresponding network configuration file.

```
# vi /etc/sysconfig/network-scripts/ifcfg-<interface>
```

   a. Change `ONBOOT=no` to `ONBOOT=yes`

   b. Change `BOOTPROTO=dhcp` to `BOOTPROTO=none`

   c. Add the line `IPADDR=172.16.0.99`

   d. Add the line `NETMASK=255.255.255.0`

   e. Add the line `GATEWAY=172.16.0.1`

   f. Save and exit the file.

5. Bring up the heartbeat interface. In the following example, `<interface>` represents the first heartbeat interface.

```
# ip link set <interface> up
```

6. Restart the network service as follows:

```
# systemctl restart network.service
```

7. Verify that the IP address is assigned to the heartbeat interface.

```
# ip addr show dev <interface>
```

   Example

```
# ip addr show dev eno1
2: eno1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1 →
000
```

```
    link/ether 28:80:23:a6:8a:54 brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.3/24 brd 172.16.0.255 scope global eno1
       valid_lft forever preferred_lft forever
    inet 172.16.0.2/24 brd 172.16.0.255 scope global secondary eno1:0
       valid_lft forever preferred_lft forever
    inet6 fe80::2a80:23ff:fea6:8a54/64 scope link
       valid_lft forever preferred_lft forever
```

Results

An IP address is assigned to a heartbeat interface on the node.

5.13.11.2.8 Add Node_02 to VA Cluster

This topic describes how to add the node to the VA cluster.

Prerequisites

— `root` user access to the VA nodes.

— `RHEL` has been installed on the node.

— The `RHEL` patches have been installed on the node.

— `WWN` of the node is added to the VA storage group.

Steps

1. Log on to the serial console of the existing Veritas Access node:

```
# ssh <va_iLo_admin>@<va_iLo_ip>
</>hpiLO-> start /system1/oemhp_vsp1
```

Note: If you are prevented from starting the session because another VSP session is running, it can be stopped using the following command.

```
</>hpiLO-> stop /system1/oemhp_vsp1
```

If logging on to VA iLo via SSH, do not initiate the SSH session while logged into the VA management console.

2. When prompted, enter the credentials for `master` user, to enter `clish`:

3. Add the node to the VA cluster using the '172.16.0.99' IP address:

```
nas> cluster add 172.16.0.99
```

If requested, enter the root password of the NAS node to set up SSH when prompted.

Note: A reboot will occur.

After the Veritas Access installation is complete, the following messages appear on the iLO remote console. These messages have no effect on the cluster and can be ignored.

```
vxdmpadm: Unknown error 4294967295

VxVM vxdisk ERROR V 5-1-558 Disk <hostname>_<node>_disk_0: Disk not
 in the configuration

VxVM vxdisk ERROR V-5-1-531 Device <hostname>_<node>_disk_0: online
 failed: Bad record name
```

4. Verify the reboot has started:

```
# su - master
> cluster show
Node State CPU(15 min) bond0(15 min)
 % rx(MB/s) tx(MB/s)
---- ----- ----------- -------- --------
node_01 EXITED
node_02 RUNNING 13.32 11.19 18.02
```

5. Verify the node has rejoined to the cluster (this can take 5-10 minutes):

```
> cluster show
Node State CPU(15 min) bond0(15 min)
 % rx(MB/s) tx(MB/s)
---- ----- ----------- -------- --------
node_01 RUNNING 3.42 1.50 3.72
node_02 RUNNING 13.32 11.19 18.02
```

6. Verify the VIPs are balanced by repeatedly running the following command until balanced:

```
> network ip addr show
IP Netmask/Prefix Device Node Type Status
-- -------------- ------ ---- ---- ------
10.1.1.2 255.255.252.0 bond0 nas551011_01 Physical
10.1.1.3 255.255.252.0 bond0 nas551011_02 Physical
10.1.1.10 255.255.252.0 bond0 nas551011_01 Virtual ONLINE (Co
n IP)
10.1.1.11 255.255.252.0 bond0 nas551011_02 Virtual ONLINE
10.1.1.12 255.255.252.0 bond0 nas551011_01 Virtual ONLINE
```

Note: `rport` messages may appear. These messages have no effect on the cluster and can be ignored.

```
rport-X:X-XX: blocked FC remote port timeout: removing port
```

7. Log on to the added node as support user.

    a. Check whether the temporary IP still exists on the Installation NIC (eth<XX> can be identified from Step 21 of Install RHEL OS on page 122.

    Note: If the temporary IP is not configured then proceed to Step 8

    ```
    # ifconfig -a eth<XX>
    ```

    Example

    ```
    nas29342936_02:~ # ifconfig -a eth1
    eth1      Link encap:Ethernet  HWaddr AC:16:2D:70:3E:BD
              inet addr:10.42.235.128  Bcast:10.42.235.255  Mask:255.25 →
    5.252.0
              inet6 addr: fe80::ae16:2dff:fe70:3ebd/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
              RX packets:6919 errors:0 dropped:0 overruns:0 frame:0
              TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:579845 (566.2 KiB)  TX bytes:1020 (1020.0 b)
              Interrupt:36
    ```

    b. If the temporary IP still exists on the NIC , then open the following file to edit the contents:

    ```
    # vim /etc/sysconfig/network-scripts/ifcfg-eth<XX>
    ```

    Example

    ```
    nas29342936_02:~ # vim /etc/sysconfig/network-scripts/ifcfg-eth1
    DEVICE=eth1
    HWADDR=AC:16:2D:70:3E:BD
    TYPE=Ethernet
    UUID=667e2a21-f1e9-41f7-8135-8ae8006aa0c4
    ONBOOT=yes
    NM_CONTROLLED=yes
    BOOTPROTO=none
    IPADDR=10.42.235.128
    NETMASK=255.255.252.0
    GATEWAY=10.42.232.1
    ```

    i. Change ONBOOT=yes to ONBOOT=no

    ii. Change BOOTPROTO=none to BOOTPROTO=dhcp

    iii. Delete IPADDR, NETMASK, and GATEWAY lines.

    iv. Save and exit the file.

    Example

    ```
    nas29342936_02 ~]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
    DEVICE=eth1
    HWADDR=AC:16:2D:70:3E:BD
    TYPE=Ethernet
    UUID=667e2a21-f1e9-41f7-8135-8ae8006aa0c4
    ONBOOT=no
    ```

```
NM_CONTROLLED=yes
BOOTPROTO=dhcp
```

8. Reboot the recently added node to complete configuration of the node:

```
nas> cluster reboot <node_name>
```

Note: Answer **y** if dedup message is shown:

```
Get dedup jobs status on nas550203_01 failed. Reboot/Shutdown may f →
ail dedup running jobs on nas550203_01.

Do you want to continue (y/n) y
```

This extra reboot is required, even though the node rebooted at the end of the add operation.

9. Check that both nodes are running (this can take 5-10 minutes):

```
> cluster show
Node State CPU(15 min) bond0(15 min)
 % rx(MB/s) tx(MB/s)
---- ----- ----------- -------- --------
node_01 RUNNING 3.42 1.50 3.72
node_02 RUNNING 13.32 11.19 18.02
```

10. Verify the VIPs are balanced by repeatedly running the `network ip addr show` command until balanced:

```
> network ip addr show
IP Netmask/Prefix Device Node Type Status
-- -------------- ------ ---- ---- ------
10.1.1.2 255.255.252.0 bond0 nas551011_01 Physical
10.1.1.3 255.255.252.0 bond0 nas551011_02 Physical
10.1.1.10 255.255.252.0 bond0 nas551011_01 Virtual ONLINE (Con IP)
10.1.1.11 255.255.252.0 bond0 nas551011_02 Virtual ONLINE
10.1.1.12 255.255.252.0 bond0 nas551011_01 Virtual ONLINE
```

11. Log out to become a support user.

12. Check that the Access NAS Configuration Kit files still exist on the node:

```
# ls /media/config
```

13. If the files still exist, then skip to Step 16 to configure the cluster:

    If necessary, create a directory to store the Access NAS Configuration Kit.

```
# mkdir -p /media/config
```

14. Download and copy the Access NAS Configuration Kit into the directory created in previous step. Check relevant deployment release note for revision information.

15. Install the Access NAS Configuration Kit by entering the following commands where <ver> represents the version of the Access NAS Configuration Kit, and <version> represents the version of the extracted RPM.

```
# cd /media/config
# tar xvf 19089-CXP9033343_X_<ver>_TAR_GZIPV1.tar.gz
# yum install ERICnasconfig_CXP9033343-<version>.rpm -y
```

16. Configure the cluster using the following commands and answer yes to all the questions.

```
# cd /media/config
# ./configure_NAS.bsh -a rpm
```

Note: Reboot may occur.

17. If a reboot did not occur in Step 16 then reboot the recently added node to complete configuration of the node:

```
nas> cluster reboot <node_name>
```

18. Verify the reboot has started:

```
# su - master
> cluster show
Node State CPU(15 min) bond0(15 min)
 % rx(MB/s) tx(MB/s)
---- ----- ----------- -------- --------
node_01 EXITED
node_02 RUNNING 13.32 11.19 18.02
```

19. Verify the node has rejoined to the cluster (this can take 5-10 minutes):

```
> cluster show
Node State CPU(15 min) bond0(15 min)
 % rx(MB/s) tx(MB/s)
---- ----- ----------- -------- --------
node_01 RUNNING 3.42 1.50 3.72
node_02 RUNNING 13.32 11.19 18.02
```

20. Verify the VIPs are balanced by repeatedly running the following command until balanced:

```
> network ip addr show
IP Netmask/Prefix Device Node Type Status
-- -------------- ------ ---- ---- ------
10.1.1.2 255.255.252.0 bond0 nas551011_01 Physical
10.1.1.3 255.255.252.0 bond0 nas551011_02 Physical
10.1.1.10 255.255.252.0 bond0 nas551011_01 Virtual ONLINE (Con IP)
10.1.1.11 255.255.252.0 bond0 nas551011_02 Virtual ONLINE
10.1.1.12 255.255.252.0 bond0 nas551011_01 Virtual ONLINE
```

Note: The node is added to the VA cluster.

21. Post NAS reboot, update the CLIENT_NAME field of the bp.conf file with it's respective physical hostname.

a. Log on to the ENM MS as the brsadm user:

```
# ssh -X -l brsadm <ms_ip_address>
```

b. Get the list of nodes connected to MS:

```
# /opt/ericsson/itpf/bur/bin/bos --operation list_nodes
```

Example:

```
[brsadm@ieatlmsxxx-1 root]$ /opt/ericsson/itpf/bur/bin/bos --operat →
ion list_nodes

Node: db-1 Hostname: ieatrcxb2447 IP address: 10.247.246.5 Backup I →
P: 10.151.24.72 Backup hostname:ieatrcxb2447-bkp1

Node: db-2 Hostname: ieatrcxb3031 IP address: 10.247.246.8 Backup I →
P: 10.151.24.75 Backup hostname: ieatrcxb3031-bkp1

Node: svc-1 Hostname: ieatrcxb3049 IP address: 10.247.246.24 Backup →
 IP: 10.151.24.73 Backup hostname: ieatrcxb3049-bkp1

Node: svc-2 Hostname: ieatrcxb3050 IP address: 10.247.246.25 Backup →
 IP: 10.151.24.74 Backup hostname: ieatrcxb3050-bkp1

Node: svc-3 Hostname: ieatrcxb2563 IP address: 10.247.246.3 Backup  →
IP: 10.151.24.70 Backup hostname: ieatrcxb2563-bkp1

Node: svc-4 Hostname: ieatrcxb2564 IP address: 10.247.246.4 Backup  →
IP: 10.151.24.71 Backup hostname: ieatrcxb2564-bkp1

Node: nas VIP IP address: 10.140.59.110 Hostname: ieatsfsx422-423mg →
t NAS Type: VA

Node: nas atsfsx422423_01 IP address: 10.140.59.106 Hostname: ieats →
fsx422-ph1

Node: nas atsfsx422423_02 IP address: 10.140.59.107 Hostname: ieats →
fsx423-ph1

Node: ms Hostname: ieatlmsxxx-1 IP address: 10.247.246.2 Backup IP:  →
10.151.24.149 Backup hostname: ieatlmsxxx-1-bkp1
```

c. Take note of the respective NAS physical hostnames from this list.

d. Log on to each NAS client and update the `CLIENT_NAME` field of the `/usr/openv/netbackup/bp.conf` file with it's respective physical hostname.

5.13.11.2.9 NAS Audit and Health Check

The NAS Audit Health Check verifies the health of the cluster and identifies any remedial steps required.

Prerequisites

— NAS is installed.

— Unity or VNX is installed.

Steps

1. Log on to the NAS management console as the support user and run the NAS Audit script.

   ```
   # /opt/ericsson/NASconfig/bin/nasAudit.py
   ```

   The script creates an HTML results file, `/home/support/audit_report/NAS_Audit_<clustername>_<date_time>.html`.

   Note: The Access NAS Configuration Kit installs the Audit script and configures the crontab file to run the script every morning at `02:00`.

2. View the audit result.

   Examine the output of the audit, and correct any errors that are identified by the audit. Warnings must be analyzed, and addressed if needed. Corrective actions are outlined at the end of the audit report.

   Note: For an ENM deployment, the NTP Service status is marked as an error. This is expected behavior. It is fixed later in the workflow, when NAS is synchronized with ENM NTP server.

Results

The NAS Audit passes without any errors and warnings have been analyzed and addressed if needed.

5.13.11.3 Set Up Cronjob to Backup NAS Configuration

This topic describes how to schedule automated daily backups of the NAS configuration to the MWS or ENM MS to a specified location. By default, backups are retained for one week before being overwritten.

Prerequisites

— Access NAS Configuration Kit is installed.

— Access to the MWS or ENM MS.

Daily backups are stored on the MWS or ENM MS in the format `<hostname>.nas.config.<date>.tar.gz` in the specified backup location.

Note: <backup_location> is specified as the following:

— For MWS: `/JUMP/nasbackups`

— For ENM MS: `/var/www/nasbackups`

Steps

1. Set up passwordless login to the MWS or ENM MS and configure the cron job by logging on to each NAS node as support user and executing the following command.

```
# /opt/ericsson/NASconfig/bin/backup_nas_tool.bsh -a <Storage
 IP address of \
MWS or ENM MS> -p <MWS or ENM MS Root Password> -d <backup_lo
cation> \
-n <number of days to retain backups>
```

2. Log on to the management console as support user. Run the following command to backup the NAS configuration, and then verify that it completes successfully.

```
# /opt/ericsson/NASconfig/bin/backup_nas_tool.bsh -a <Storage
 IP address of MWS or ENM MS> \
-d <backup_location> -n <number of days to retain backups> -b
```

3. Verify that the log file has been created by executing the following command as support user on each NAS node.

```
# cat /opt/VRTSnas/log/backup_nas.log
```

4. Verify that the cronjob is configured by executing the following command as support user on each NAS node.

```
# crontab -l | grep "backup_nas_tool.bsh"
```

Expected Output:

```
25 02 * * * /opt/ericsson/NASconfig/bin/backup_nas_tool.bsh -
a <Storage IP address  \
of MWS or ENM MS> -d <backup_location> -n <number of days to
retain backups> -b
```

Note: Check there are no duplicate backup job enties.

If there are, then run:

```
crontab -e
```

and remove any duplicates.

Results

The NAS configuration backup is automated.

5.13.12 Reinstall HPE Blade

In the event of an OS or software failure of a server that is already deployed in a cluster, it is possible to reinstall the server without having to restore the full deployment.

Note: If more than one server is faulty in the deployment or if the server is a Database server, then a full restore of ENM is necessary.

Prerequisites

— Only one peer server in the ENM deployment is faulty, and it is faulty because of an OS or software failure.

— Peer server is not a Database server.

— Hardware is not faulty.

— Cluster contains more than one peer server.

Steps

1. Power down the server that you want to reinstall.

   Note: If the server is powered down already, skip this step.

   ```
   [root@node-1 ~]# shutdown -h 0
   ```

2. Log on to the ENM MS as the litp-admin user and switch to the root user.

3. Restore the LITP model:

   ```
   [root@ms-1 ~]$ litp restore_model
   ```

   When the command is complete, all item types in the model and deployment are in an `Applied` state.

4. Prepare the required server for a LITP restore.

   In the command example, replace `/deployments/enm/clusters/svc_cluster/nodes/svc-2` with the path to the server to be reinstalled:

   ```
   litp prepare_restore -p /deployments/enm/clusters/svc_cluster/nodes/svc-2
   ```

5. Create and run the LITP plan and wait for it to complete:

   ```
   litp create_plan
   litp run_plan
   ```

6. Configure and verify the reinstalled peer server. After reinstalling the peer server, complete the following steps:

   a. Verify that you can connect to the reinstalled peer server from the MS using SSH:

      ```
      ssh <USER>@<peer-server-ip-address>
      ```

      Note: The SSH connection to the reinstalled peer server may fail with a message similar to the following:

      ```
      RSA host key for node1 has changed and you have
      requested strict checking. Host key verification
      failed.
      ```

      If you receive this message, then edit the `/root/.ssh/known_hosts` file and remove the RSA key for the reinstalled peer server.

      Rerun the command:

      ```
      ssh <USER>@<peer-server-ip-address>
      ```

   b. Configure passwords on the reinstalled peer server.

      For more information, refer to *Configure Passwords on ENM Servers* in the ENM Installation Instructions.

7. Perform an ENM system health check:

   ```
   /opt/ericsson/enminst/bin/enm_healthcheck.sh
   ```

   If the ENM system health check script fails the VCS Service Group Healthcheck, refer to *VCS Service Group Failure* in the ENM Troubleshooting Guide. If the script reports any other errors, contact Ericsson Local Support.

8. Perform **Update ENM Backup Policies** from ENM Backup and Restore System Administrator Guide [15] to add the BRS and NetBackup Configuration to the reinstalled blade.

5.13.13 WAN-SDN Controller Hardware Management

Note: Only trusted users must be provided with the credentials to log on to the VP WAN-SDN application.

5.13.13.1 WAN-SDN Host Patching

For details of host patching please refer to the *WAN-SDN Controller Installation Guide*, available from local Ericsson support.

5.13.13.2 WAN-SDN Controller Power Down Procedure

Steps

1. Logon to the WAN-SDN Host:

```
# ssh <WAN-SDN Host IP address>
```

2. List all the guests running in the WAN-SDN Host:

```
root@wansdnhost# virsh list
```

3. Logon to the NorthStar Guest:

```
root@wansdnhost# virsh console <northstar guest vm name or ID>
```

4. Stop all the NorthStar Application services:

```
root@northstarguest# systemctl stop northstar
```

5. Check Northstar service(s) status:

```
root@northstarguest# systemctl status northstar
```

6. Exit from the NorthStar guest:

```
root@northstarguest# logout
```

or

```
ctrl+5
```

7. Shutdown NorthStar guest from WAN-SDN Host:

```
root@wansdnhost# virsh shutdown <northstar guest vm name or I →
D>
```

8. Shutdown Junos guest:

```
root@wansdnhost# virsh shutdown <Junos guest vm name or ID>
```

9. Shutdown WAN-SDN Host:

```
root@wansdnhost# shutdown -h 0
```

Results

The faulted rack is shut down.

5.13.13.3 WAN-SDN Controller Rack Replacement

> Replacing a faulted HPE rack server in a WAN-SDN Controller Deployment.

Prerequisites

— Root Access to the faulted rack.

— Access to the following information for the new rack server:

- UUID
- MAC addresses for each interface
- iLO IP address

Required Tools and Equipment

The replacement rack server has the same characteristics as the faulted rack server, including NIC cards, and is part of the same subnet.

Steps

1. Power down the rack by following the instructions in WAN-SDN Controller Power Down Procedure on page 142
2. Refer to the following sections in WAN-SDN Controller Installation Guide (available from local Ericsson support) for details on how to prepare the new rack server for installation:

Table 20 Installation Stages

Stage	Section
Ethernet cabling	Connect Gen10 Rack Server to Ethernet
iLO configuration	Configure the iLO IP Address
iLO Licenses	Add iLO Licenses to HPE ProLiant Rack Servers
BIOS Procedures	BIOS Procedure

5.13.13.4 WAN-SDN Controller Blade Replacement

5.13.13.4.1 Shutdown the Faulted Blade

Note: If possible, check the firmware levels on the faulted blade before shutting it down.

Steps

1. Log on as the root user to the iLO of the faulted blade.
2. Start the Virtual Serial Port (vsp) service:

```
hpiLO-> vsp
```

3. Power down the faulted node:

```
[root@node ~]# shutdown -h 0
```

4. If the vsp service is unresponsive in step 2, then shut down the faulted blade from the iLO:

```
hpiLO-> power off hard
```

5. Check the power status of the faulted blade.

```
hpiLO-> power
```

Results

The faulted blade is shut down.

5.13.13.4.2 Replace the Faulted Blade with the Replacement Blade

When the faulted blade is powered down, contact HPE Support to remove the faulted blade from the enclosure, and insert the replacement blade into the same bay.

Note: For hardware commissioning and backup and restore to work with the replacement blade, you must insert it into the same bay as the faulted blade.

Result

The replacement blade is inserted into the enclosure.

5.13.13.4.3 Check Replacement Blade Firmware

Check that the blade and NIC firmware are at the levels specified by the FLARE and Firmware Handling Guide for HP/EMC (available from local Ericsson support).

Result

The blade firmware and NIC firmware are at the required levels.

5.13.13.4.4 Configure Replacement Blade BIOS Settings

Complete the *BIOS Procedure* in the WAN-SDN Controller Installation Guide (available from local Ericsson support) for BIOS settings

Apply WAN-SDN Controller specific commissioning procedure and installation according to WAN-SDN Controller Installation Guide.

Result

Replacement blade BIOS settings are configured.

5.14 Update the External NTP Servers in ENM

> How to update the NTP server list of different systems in the ENM deployment.

The ENM Management Server, the esmon VM, and all peer servers of the Service Cluster can be configured to use up to three external NTP servers specified in the Site Engineering Document - ntp_1_IP, ntp_3_IP, and ntp_4_IP.

All VMs in the ENM deployment can be configured to use only one external NTP server specified in the Site Engineering Document – the ntp_1_IP value.

The NTP server list of the peer servers of all other clusters cannot be configured to use any external NTP server.

Note: The ENM deployment uses a modeled configuration and timing is critical for the core of the system. The following steps are mandatory for updating the external NTP servers in ENM.

Prerequisites

— External NTP servers are IP contactable over the services VLAN Network.

— The Site Engineering Document is available for updates.

Steps

1. Update any, or all, of the ntp_1_IP, ntp_3_IP, and ntp_4_IP values in the Site Engineering Document with the new NTP IP addresses.
2. Perform a model-only upgrade, or an overall ENM upgrade.

   For more information about upgrading ENM, see *Upgrade ENM* of the ENM Upgrade Instructions.
3. Check that the NTP servers are updated correctly:

   a. Log on to the MS as the `litp-admin` user and switch to the `root` user.

   b. Use the following commands to check the NTP services on the required nodes:

   #### ENM Management Server

   ```
   # /usr/sbin/ntpq -pn
   ```

   #### SVC Peer Server

   ```
   # ssh litp-admin@<svc_peer_server_name>"/usr/sbin/ntpq -pn"
   ```

   #### VMs

   ```
   # ssh -i /root/.ssh/vm_private_key cloud-user@<vm-name>"/usr/sbin/n
   tpq -pn"
   ```

   The `ntpq` command outputs a list and summary of the state of the peer servers known to the server.

   Example

   ```
   [root@cloud-ms-1 ~]# ntpq -pn
        remote           refid      st t when poll reach   delay   off
   set  jitter
   ==============================================================
   ===========
   *159.107.173.12  193.180.251.38   3 u  768 1024  377    1.476   -0.
   664   0.799
   ```

```
 172.16.30.19    .INIT.          16 u    - 1024    0    0.000    0.
000   0.000
+192.168.0.1     159.107.173.12   4 u  660 1024  377    0.289    0.
507   0.622
 127.127.1.0     .LOCL.          10 l   4d   64    0    0.000    0.
000   0.000
```

In the previous example:

- The `remote` column lists the NTP servers and must match the SED values.
- The first line shows that a remote server is synchronized as there are values present in each column. The * sign at the beginning indicates that it is the main NTP server in use.
- The second line shows that an NTP server is not synchronized. The refid state is .INIT. for initializing and indicates that the remote server has no reference. All other column values are zero.
- The third line shows that a remote server is synchronized. The + sign on the beginning indicates that it is a candidate peer server.

c. Verify that the outputs are correct using the NTP server list and the updated SED values.

Results

On completion of the ENM upgrade, the NTP server list of ENM Management Server, esmon VM, and SVC Peer Servers are updated with the new values of ntp_1_IP, ntp_3_IP, and ntp_4_IP.

The NTP server list of all other VMs is updated to reflect any new value of ntp_1_IP. The NTP server list of all other Peer servers remain unaffected.

5.15 Change EMC Password in LITP Model

> After you change the EMC password on the EMC SAN, use the following procedure to change the EMC SAN password in the LITP model.

Prerequisites

You have changed the EMC password on the EMC SAN.

Steps

1. Log on to ENM MS as the `litp-admin` user, then switch to the root user.
2. Find the name of the key and user.

```
litp show -p /infrastructure/storage/storage_providers/san1/| grep -e key -e
 username
```

```
username: admin
password_key: key-for-san-ieatvnx-99
```

3. Update the LITP model, if the name of the user has changed.

```
litp update -p /infrastructure/storage/storage_providers/san1 →
/ -o username=<new user>
```

   The SAN item remains in an updated state until a LITP plan is run.

4. Delete the old password credentials from the LITP model.

```
litpcrypt delete <password_key> <username>
```

5. Add the new password credentials.

```
litpcrypt set <password_key> <username> <password>
```

5.16 Configure SAN Data Collection

This section describes the procedure to check the performance metrics collection is enabled on the SAN. If degraded SAN performance is observed during ENM runtime, this data can be analyzed to determine the root cause.

Steps

For Unity, do the following:

— Configure Performance Data Collection on Unity

For VNX, do the following:

— Configure NAR Data Collection on VNX

5.16.1 Configure Performance Data Collection on Unity

The performance metrics collection service is enabled by default. This is a procedure to verify that metrics collection is enabled, if the metrics collection is not enabled steps are given to enable the metrics collection. If degraded Unity performance is observed during ENM runtime, this data can be analyzed to determine the root cause.

Prerequisites

— Initial installation of the ENM MS has taken place.

— Initial commissioning of Unity has taken place.

Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. Check the current status of the metrics collection service.

```
[root@ms]# /usr/bin/uemcli -d <sp_ip> /metrics/service show
```

Example:

```
[root@ms ~]# /usr/bin/uemcli -d 10.45.22.54 /metrics/service show
Storage system address:10.45.22.54
Storage system port: 443
HTTPS connection
)
1:    History enabled    yes
      History retention = 2019-04-27 12:48:00 (60 sec), 2019-04-16 16:00:00
(300 sec), 2019-04-04 00:00:00 (3600 sec), not available (14400 sec)
```

Note: If the output from the command show history enabled is yes, no further action is needed.

If the output from the command does not show history enabled as yes, continue to Step 3.

If the data for a certain interval is not yet available, the system displays not available instead of a time stamp.

3. Enable historical metrics collection service.

```
[root@ms ~]# uemcli -d 10.45.22.54 /metrics/service set -historyEnabled yes
```

4. Confirm that the metrics collection is enabled.

```
[root@ms]# /usr/bin/uemcli -d <sp_ip> /metrics/service show
```

Example:

```
[root@ms ~]# /usr/bin/uemcli -d 10.45.22.54 /metrics/service show
Storage system address:10.45.22.54
Storage system port: 443
HTTPS connection

1:    History enabled    yes
      History retention = 2019-04-27 12:48:00 (60 sec), not available (300 s
ec), not available (3600 sec) not available (14400 sec)
```

5.16.2 Configure NAR Data Collection on VNX

Enabling NAR data collection on the VNX storage array during ENM installation is recommended. This is a one-time procedure that enables collection of VNX performance data. If degraded VNX performance is observed during ENM runtime, this data can be analyzed to determine the root cause.

Prerequisites

- VNX is initialized
- SP IP addresses are configured and available
- VNX administration user is created
- VNX `Unisphere` Analyzer enabler is installed
- User security file is created

Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. Check the analyzer settings on the storage array:

```
[root@ms]# naviseccli -h <SPA> analyzer -get
```

Example:

```
[root@ms]# naviseccli -h 10.32.229.46 analyzer -get
Archive Poll Interval (sec):  60
Real Time Poll Interval (sec):  60
Periodic Archiving:  Yes
Current Logging Period (day):  nonstop
```

Note: If the output from the command does not match the example, continue to Step 3.

If the output from the command matches the example, continue to Step 2a.

a. Verify the analyzer status on each SP:

```
[root@ms]# naviseccli -h <SPA> analyzer -status
[root@ms]# naviseccli -h <SPB> analyzer -status
```

Example:

```
[root@ms ~]# naviseccli -h 10.32.229.46 analyzer -status
```

```
Running. Started on 02/06/2018 09:52:34
[root@ms ~]# naviseccli -h 10.32.229.47 analyzer -status
Running. Started on 02/06/2018 09:52:34
```

If the analyzer is not Running on either SP, run the following command on each affected SP to enable it:

```
[root@ms ~]# naviseccli -h <SP> analyzer -start
```

b. Verify that statistics logging is enabled:

```
[root@ms]# naviseccli -h <SPA> setstats
```

Example:

```
[root@ms ~]# naviseccli -h 10.32.229.46 setstats
Statistics logging is ENABLED
```

If statistics logging is not enabled, run the following command to enable it:

```
[root@ms]# naviseccli -h <SPA> setstats -on
```

Note: The procedure is complete. Do not perform any further steps in the procedure.

3. Apply the analyzer settings and start the analyzer:

```
[root@ms ~]# naviseccli -h <SPA> analyzer -set -narinterval 60 -rtinterval 6 →
0 -periodicarchiving 1 -nonstop
[root@ms ~]# naviseccli -h <SPA> analyzer -start
```

4. Confirm that the correct analyzer settings are applied:

```
[root@ms]# naviseccli -h <SPA> analyzer -get
```

Example:

```
[root@ms]# naviseccli -h 10.32.229.46 analyzer -get
Archive Poll Interval (sec):  60
Real Time Poll Interval (sec):  60
Periodic Archiving:  Yes
Current Logging Period (day):  nonstop
```

5. Enable statistics logging and verify that it is enabled:

```
[root@ms]# naviseccli -h <SPA> setstats -on
[root@ms]# naviseccli -h <SPA> setstats
```

Example:

```
[root@ms ~]# naviseccli -h 10.32.229.46 setstats -on
[root@ms ~]# naviseccli -h 10.32.229.46 setstats
Statistics logging is ENABLED
```

5.17 Configure User Quotas for Shared Home Area

> This task describes how to set quotas for POSIX (Portable Operating System Interface) users on the Ericsson Network Manager (ENM) system.

This `user quota` for NAS solution is installed by default to ENM scripting cluster during installs, upgrades and restores.

This procedure is only applicable to, and performed by, an ENM user with the prerequisite UNIX administrative access. Every regeneration of a Scripting VM image will generate a new host SSH key so successful (manual or automated) execution of the quota script requires the prerequisite step of exchanging the SSH keys of the scripting node, where the quota script is to be executed, with both NAS system hosts as required.

The `user quota` for NAS solution will enable configuration of quotas for all POSIX users. The defined default quota is supplied as an argument to the quota script, and the defined personalized per-user quotas are defined in a user-quota configuration file. During execution of the quota script, the creation time of each user is compared to the time of the last run of the quota script (a time-stamp file) and only newer users are enforced with this default quota. On first execution, all users have the quota applied. On subsequent execution, only new users have the quota applied. The following User Cases are supported:

Default Quota - all existing POSIX users

Every current user is governed by the default quota value, specified as an argument to the first (manual or automated) execution of the quota script.

Default Quota - all new POSIX users

Subsequent newly-created users are not governed by any default quota until after the next successful (manual or automated) execution of the quota script with the required default quota value as argument. The same default quota value must be enforced between all subsequent executions of the quota script (varying the default quota value between subsequent executions is supported but it is not intuitive).

Revised Default Quota - all existing POSIX users

Every current user can be governed by a revised default quota value, after both the deletion of the time-stamp file and the next successful (manual or automated) execution of the quota script with the revised default quota value as argument.

Per-User quota - any existing POSIX users

Every current user is governed by the current personalized quota value, defined for that user in the documented user quota file, after the next subsequent and successful (manual or automated) execution of the quota script.

Per User quota, where defined for that user, has precedence over default quota value.

Prerequisites

— Root user access to scripting VM.

— `master` and `support` passwords for the NAS.

5.17.1 Configuration

5.17.1.1 Enable Quotas for the NAS Filesystem

> Enable Quotas for the NAS Filesystem

1. Execute the `storage quota fs enable <filesystem>` command on the NAS system.

   — In a typical deployment, the file system for ENM POSIX users is named `enm-home`.

   — Connect to NAS as the `master` user.

   — Run the command on NAS CLISH.

   Example

```
NAS>storage quota fs enable enm-home

NAS> storage quota fs status enm-home
FS name                   User Quota   Group Quota
=======                   ==========   ==========
enm-home                  Enabled      Enabled
Command completed successfully
```

5.17.1.2 Create a new host SSH key

The regeneration of a Scripting VM image creates a new host SSH key. This procedure is applicable to ensure the Scripting VM can access the NAS system by sharing this public key for the root user.

Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. Log on to scripting VM Server as cloud-user.

```
# ssh -i /root/.ssh/vm_private_key cloud-user@scp-1-scripting
```

3. Switch to root user

```
[cloud-user@scp-1-scripting ~]$ sudo su root
```

4. Generate the SSH key on the scripting VM Server as the root user, by executing the `ssh-keygen` command to generate a private/public key pair (accept defaults by pressing ENTER at each prompt).

   Example

```
[root@scp-1-scripting ~]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
1a:3c:80:a1:d1:20:d9:6f:51:a7:e3:99:59:57:80:35 root@scp-1-scripting
The key's randomart image is:
+--[ RSA 2048]----+
|+=.  .. .oE..    |
|oooo.  o.  o     |
|. ....o . .      |
|    o+ * .       |
|   .  O S        |
|      +          |
|      .          |
|                 |
|                 |
+-----------------+
```

5. Copy the public key of the root user to both NAS nodes.

   a. Retrieve the IP addresses of both NAS nodes:

```
[root@scp-1-scripting ~]#mount | grep ericsson | gawk -F ":" '{prin →
t $1}' | sort | uniq
10.10.0.10
10.10.0.11
```

   b. Run the following command for both IP addresses that were returned in the previous command (you will be prompted):

```
[root@scp-1-scripting ~]# ssh-copy-id support@10.10.0.10
[root@scp-1-scripting ~]# ssh-copy-id support@10.10.0.11
```

c. Verify with the SSH command that it is possible to log on to the NAS nodes without prompting for password:

```
[root@scp-1-scripting ~]# ssh support@10.10.0.10
[root@scp-1-scripting ~]# ssh support@10.10.0.11
```

5.17.2 Enable Quotas

5.17.2.1 Enforce System Default Quota

Enforce a default quota on all POSIX users that are not using per-user quotas.

Steps

1. Configure the system default user quota by running the `set_quota.sh <quota>` command using following recommendations:

   — The `<quota>` argument is a numeric value followed by the size identifier (K - Kilobytes, M - Megabytes, G - Gigabytes).

   — The default quota is assigned to all POSIX users not defined in the user-quota configuration file and added since the last run of this same quota script.

   — After a successful run of the quota script, the timestamp file is created at `/ericsson/tor/no_rollback/quotas/timestamp`.

   — To change the default quota, delete this timestamp file first.

   Example

   ```
   [root@scp-1-scripting ~]# /ericsson/ERICenmsggeneralscripting_CXP9031992/bin →
   /set_quota.sh 10M
   ```

2. Optionally, execute the quota script by CRON by running the `crontab -e` command.

   a. Use root cronjob.

   b. On subsequent jobs, the quota command is only enforced on new users, omitting users who had the quota already set up.

   c. On a system with multiple scripting nodes, enable the quota script on one scripting node only.

   Example

   Refer to the following:

```
59 2 * * * /ericsson/ERICenmsggeneralscripting_CXP9031992/bin/set_q →
uota.sh 10M > /dev/null 2>&1
```

3. If required, review system messages in the `/var/log/messages` directory for problems reported by the `set_quota.sh` script.

5.17.2.2 Enable Per-user Quotas

> Optionally enable per-user quotas. This allows ENM users to have different limits on their disk usage.

1. Configure the per-user quota in the `/ericsson/tor/no_rollback/quotas/users` configuration file.
   - Use the following format for per-user quota: `"username":"quota"`.
   - The quota identifier represents the amount of quota assigned to the user.
   - Lines beginning with the # character are considered as comments and are ignored.

   Example

   ```
   # Users file defining the individual quota per user
   # the format is following:
   #  "username":"quota"
   #   - quota is in the same format as in SFS
   #    Numeric value followed with identifier
   #     K - Kilobyte
   #     M - Megabyte
   #     G - Gigabyte
   administrator:200M
   ```

2. Per user quotas are enforced by running the `set_quota.sh <quota>` command.

   In the following example, the `set_quota.sh` script accepts the argument that is the default quota value for all users.

   ```
   [root@scp-1-scripting ~]# /ericsson/ERICenmsggeneralscripting_CXP9031992/bin →
   /set_quota.sh 10M
   ```

5.17.3 Disable the User Quota for NAS

> The following section outlines how to disable the user quota for NAS solution.

1. Disable quotas on the NAS system by running the `quota fs disable <filesystem>` command.

a. Connect to the NAS system as `master` user.

   The name of the file system is `enm-home` by default.

Example

```
NAS>storage quota fs disable enm-home
Command completed successfully
```

2. Disable any `set_quota.sh` crontab job for the root user using the `crontab -e` command from all scripting VM.

5.18 Configure VLAN and Multicast Settings

ENM deployments are IP dual-stack and support both IPv4 and IPv6 traffic regardless of the network type or protocols for the managed network.

To receive IPv6 multicast traffic, an IPv6 host (physical or virtual) must explicitly join a multicast group by sending a Multicast Listener Discovery (MLD) report. MLD is the protocol used by an IPv6 host to register its IP multicast group membership with a router and the router will then forward traffic to that host.

An MLD querier sends out periodic MLD queries that trigger MLD report messages from the hosts (physical or virtual) that want to receive IP multicast traffic. MLD snooping listens to these MLD reports to establish appropriate forwarding.

In ENM deployments multicast traffic is used for internal communications between software components on the Internal and Jgroups VLANs. As this is Layer 2 switched, an IP-multicast router is not required. However, the switch must be configured so that it acts as a multicast querier towards the software bridges on the ENM host blades. These are configured to use MLD snooping and require a querier to forward multicast traffic appropriately.

Multicast Bridge Properties

— The `multicast_snooping` property is used to enable or disable multicast snooping. The value of the property must be `0` (disabled) or 1 (enabled).

— The `hash_max` property sets the size of the multicast hash table within the Linux kernel. The value of this property is environment specific.

— This `multicast_querier` property is used to enable or disable multicast querier. The value of the property must be `0` (disabled) or 1 (enabled).

— The `multicast_router` property is used to specify if ports have multicast routers attached.

  — The value of `0` disables this property completely.

  — The value of 1 allows the system to automatically detect the presence of routers.

— The value of 2 means ports will always receive all multicast traffic.

5.18.1 Configure Switch Settings for the Services VLAN

The following settings must be configured on the Services VLAN:

— MLD is enabled

— Multicast snooping is disabled

5.19 Neo4j Backup and Consistency Check on Physical

This task lists the steps that should be followed to create a Neo4j Database backup on a Physical Server and run the Neo4J Consistency Check on this database.

This is relevant for ENM Physical (Neo4j Causal Cluster and Neo4j Single Instance).

This is an emergency procedure. Typically the Neo4j Backup and Consistency Check is performed as part of the overall BUR/OMBS Backup and this is adequate. However, you are provided with a utility to manually run a Neo4j Backup and Consistency Check.

Be aware that the space required to accommodate the Neo4j Backup needs to be at least as big as the current Neo4j Graph Database!

Prerequisites:

— DB node(s) are installed and Neo4J is running in the appropriate DB nodes.

— Root access to the DB nodes.

— Adequate disk space greater than the size of Neo4j database available in the Local File System for storing backup.

Expected Result:

A Neo4j backup file, produced during the backup process, will be automatically removed by this process, following a successful consistency check.

Note: In ENM we do not support Neo4J Database Restore. The supported restore is via snapshot and includes associated DB Systems e.g. PostgreSQL.

We also support full restore via OMBS.

For more information for Restore, refer to BUR documentation and for Rollback, refer to the relevant Upgrade Documentation.

5.19.1 Manual - Backup and Consistency Check Procedure

1. If on a Single Instance server, log in to the db node where Neo4j is offline, then switch to the root user; if on a Causal Cluster server, log in to db-1, then switch to the root user.

2. To run a backup and consistency check procedure and delete the backup file after a successful procedure, run the following command:

```
[root@hostname ~]# /opt/ericsson/neo4j/backup_and_cc/backup_cc.py
```

Note: The backup directory/files will NOT be deleted automatically if this procedure fails for any reason. In such scenario, manually delete the directory immediately after the failure or after analysis/ troubleshooting (if required).

The backup will fail if there is a failover of Neo4j during the backup procedure on ENM Large or ENM Medium deployments (Single Instance Neo4j deployments).

The manual backup procedure will fail if OMBS backup is currently running, or if OMBS backup is triggered before the manual backup is completed.

The space available in the directory to be used for storing the backup file must be at minimum the size of the Neo4j database file that backup would be taken from. If a directory with insufficient space is used then a validation error message showing the required and available space will be printed, see example following:

```
[root@hostname ~]# /opt/ericsson/neo4j/backup_and_cc/backup_cc.py --dir /var/tmp/
 Running validations before Backup
 Insufficient space for storing backup in /var/tmp/. Space required is 181.79G, but only 8.67G is available
```

If the default directory is used for storing backup on a Single Instance Server, and the directory does not exist on the offline DB node, then an error message similar to the following will be received: "Neo4j backup/CC did not run because the specified backup directory /ericsson/neo4j_bur/ does not exist". Then perform the procedure in Switch Neo4j BUR LUN on Single Instance on page 160 .

3. To run the backup and consistency check procedure with the option of storing the backup file, run the following command:

```
[root@hostname ~]# /opt/ericsson/neo4j/backup_and_cc/backup_cc.py --store-backup
```

This would be relevant if ENM Support or Neo4J require a copy of the specific database for troubleshooting.

5.19.2 Switch Neo4j BUR LUN on Single Instance

Note: This section is applicable to Neo4j Single Instance Servers only.

Where the default directory for storing backup does not exist in the offline db node, and on executing the manual Backup/CC script, an error message similar to the following is received: "Neo4j backup/CC did not run because the specified backup directory /ericsson/neo4j_bur/ does not exist", then perform the following steps to switch the Neo4j BUR LUN (/ericsson/neo4j_bur) to the offline directory:

Steps

1. Log on to the DB node where Neo4j is online, then switch to the root user.
2. Run the following command, then enter the number beside <Grp_CS_db_cluster_sg_neo4jbur_clustered_service> as in the printout below:

```
[root@hostname ~]# /opt/ericsson/neo4j/util/dps_db_admin.py s →
witch

         ############        WARNING        ############
           This option should not be executed during
                 an Upgrade or Initial Install.
         ############        WARNING        ############

Groups available for switching:

        1 Grp_CS_db_cluster_jms_clustered_service
        2 Grp_CS_db_cluster_postgres_clustered_service
        3 Grp_CS_db_cluster_elasticsearch_clustered_service
        4 Grp_CS_db_cluster_sg_neo4jbur_clustered_service
To exit without switching, use CTRL+C.
To switch groups, enter relevant number(s) (1 to 5) from the  →
list above with each number separated by space or leave blank →
 to switch all groups: 5
 Switching Grp_CS_db_cluster_sg_neo4jbur_clustered_service, p →
lease wait...
 Grp_CS_db_cluster_sg_neo4jbur_clustered_service has been suc →
cessfully switched.
 Switch procedure has been completed.
```

3. Confirm that a message similar to: "Grp_CS_db_cluster_sg_neo4jbur_clustered_service has been successfully switched" is seen in the updated output.

   Result: The Neo4j BUR LUN (/ericsson/neo4j_bur) is now available for storing backup in the offline DB node.

5.19.3 Default Parameters and How to Change Them

1. Below are a list of default parameters that can be changed:
   - Default Backup Directory Single Instance: `/ericsson/neo4j_bur`
   - Default Backup Directory Causal Cluster: `/ericsson/neo4j_data`
   - Default Backup Name: `backup_graph.db`
2. Changing default parameters:
   - To specify a custom backup directory: --dir=<target_directory>

     Note: Backup directory that is used must be located in the Local File System. (To see Filesystem list, run command: 'df -h'. Local Filesystems would usually start with '/dev/')
   - To specify a custom backup name: --name =<backup_name>
3. Examples of how to specify custom parameters:
   - To change the backup name:

```
[root@hostname ~]#/opt/ericsson/neo4j/backup_and_cc/backup_cc.py --stor →
e-backup --name=graph.db_backup_21_09_18
```

Note:
a. Do not run Backup & Consistency Check during ENM Upgrades, or during any optional workload procedures like Troubleshooting

b. An "Exception" similar to "causalclustering.catchup.storecopy.StoreCopyClient" may be seen if trying to execute the script at a time when the DB node is restarting or changing role.

   In such cases, you should retry again after a few minutes.

5.19.4 Additional Parameters for Backup and Consistency Check

The following additional parameters may be used when running Backup and Consistency Check:

Parameter Name	Description	Default
--disable-cc	Use this argument to disable the execution of Consistency Check after backup.	Consistency Check is enabled.
--store-backup	Use this argument to store the backup files after the backup operation.	Backup files are deleted, except the Backup or Consistency Check execution fails.
--enable-debug	Use this argument to see the debug output during Backup or Consistency Check operation. This option is useful for debugging and troubleshooting.	Debug output is disabled.

5.20 Configure ENM Email Relay Service to Add Routing Notifications via Email

Update ENM Email Relay Service to route network notifications via email.

Prerequisites

Root user access to the ENM MS and LITP

Steps

1. Update ENM SED variable `EMAIL_DOMAIN` to a domain, relayhost alias, or specific IP address.

    a. Log on to the ENM MS (ms-1) as the `litp-admin` user, switch to `root`, and then log on to the ENM `lvsrouter`.

    If password authentication is disabled for the `litp-admin` user, then refer to *Log On to the MS when Password Authentication is Disabled* in the *LITP Node Hardening Instructions*.

    ```
    # ssh litp-admin@ms-1

    # su -

    # ssh -i /root/.ssh/vm_private_key cloud-user@svc-1-
    lvsrouter
    ```

    b. Verify current `EMAIL_DOMAIN` value.

    ```
    # cat /ericsson/tor/data/global.properties | grep
    EMAIL_DOMAIN
    ```

    EMAIL_DOMAIN=<current_value>

    c. Update the `EMAIL_DOMAIN` attribute in the litp model.

    ```
    # exit

    # litp update -p /software/items/config_manager/
    global_properties/EMAIL_DOMAIN -o
    value=<new_email_domain_value>
    ```

    d. Create and run the litp plan

    ```
    # litp create_plan

    # litp run_plan
    ```

    e. Once plan finishes successfully, verify that value has been updated:

```
# watch -n 5 litp show_plan

# cat /ericsson/tor/data/global.properties | grep
EMAIL_DOMAIN
```

EMAIL_DOMAIN=<new_email_domain_value>

2. Offline, undefine and online lvsrouter VM.

    a. To start with offline lvsrouter - ssh to svc-1

    ```
    # ssh litp-admin@cloud-svc-1
    ```

    b. change to root and check the status of lvsrouter cluster in SVC-1

    ```
    # su

    # hagrp -state | grep lvsrouter
    ```

    c. Offline lvsrouter cluster

    ```
    # hagrp -offline Grp_CS_svc_cluster_lvsrouter -sys
    <name of svc>
    ```

    d. Check the current state of lvsrouter expecting offline

    ```
    # watch -n 5 "hagrp -state | grep lvsrouter"
    ```

    e. Once lvsrouter clusters are offline, undefine (delete) them.

    In SVC-1 as root verify lvsrouter is shut off and undefine the VM

    ```
    # virsh list --all

    # virsh undefine lvsrouter
    ```

    f. Re-verify if lvsrouter has been removed or not, expected output : lvsrouter details should not appear in the list.

    ```
    # virsh list --all
    ```

    g. Online svc-1 lvsrouter again from svc-1 itself as:

    ```
    # hagrp -online Grp_CS_svc_cluster_lvsrouter -sys <name
    of svc>
    ```

    h. Check the current state of lvsrouter expecting online:

    ```
    # watch -n 5 "hagrp -state | grep lvsrouter"
    ```

    i. ssh onto SVC-2 (you have to go in each SVC cluster to delete lvsrouter), repeating steps a to h for each SVC.

3. Verify that the value in `global.properties` file was updated on the lvsrouters.

If password authentication is disabled for the litp-admin user, then refer to *Log On to the MS when Password Authentication is Disabled* in the *LITP Node Hardening Instructions*.

```
# ssh litp-admin@ms-1

# su -

# ssh -i /root/.ssh/vm_private_key cloud-user@svc-2-lvsrouter

# cat /etc/postfix/main.cf | grep ^relayhost
```

relayhost = new_email_domain_value

Optional:

4. To send Email from a VM.

```
echo "Test Body" | mailx -v -s "Subject" -S smtp="emailrelay:25" <username@d →
omain.com>
```

Results

The email relay service is configured to forward email to the updated destination.

5.21 Reduce System Usage for /ericsson/batch/ File System for Bulk Export

The `/ericsson/batch/` file system for Bulk Export may grow and require maintenance.

If the `/ericsson/batch/` file system exceeds 90% capacity in a physical deploment, the export feature is unable to export files. Reducing the `/ericsson/batch/` file system usage below this threshold re-enables the export feature.

Prerequisites

— Access to the ENM Command Line Interface (CLI), with permissions to remove export jobs, if the capacity of the `/ericsson/batch/` file system is up to 90%.

— Access to the Server Cluster (SVC) nodes, if the capacity of the `/ericsson/batch/` file system is up to 90% (physical deployment only).

— Access to the Ericsson Management Portal (EMP) VM (cloud deployment only).

— Username and password for the shared file system (SFS), if the capacity exceeds 90%. (physical deployment only).

— A list of job IDs of the export jobs or files which can be deleted.

— A backup of the export files exists in a location external to the ENM deployment, if required.

Steps

1. Check the space available on the `/ericsson/batch/` file system by running the following commands. Regularly check the free space and delete old files and sub-directories as needed.

    a. On a physical deployment, run the following command from any of the SVC nodes:

    ```
    [ root@<svc-hostname> ~]# df -h | grep batch
    <SVC_NODE_IP>:/vx/lms999-batch
                          10G  423M  9.0G   5% /ericsson/batch
    ```

    b. On a cloud deployment, run the following command from the EMP VM:

    ```
    [root@gat-emp-0 ~]# df -h | grep batch
    nfsbatch:/ericsson/batch               9.8G   43M  9.2G   1% /eric →
    sson/batch
    ```

    Note: If the `/ericsson/batch/` file system space available is above 90% on a physical deployment, follow steps 4 to 9.

    Otherwise, on both physical and cloud deployments, follow step 2 to 3.

2. Log on to ENM and launch the Command Line Interface.

3. Run the following command to delete an export job, which will remove the job and associated bulk CM export file.

    ```
    cmedit export -rm -j <job-id>
    ```

    Note: When you delete the job with `<job_id>`, you cannot download the Bulk Export file using the download command for the particular job ID. Therefore, you must download any required export files in advance of this operation.

4. Repeat from step 1 until the capacity of the `/ericsson/batch/` file system is at less than 80%. If the capacity is now less than 80%, do not proceed to step 4.

5. If the `/ericsson/batch/` file system on a physical deployment is over 90% capacity, its state changes to `Read-only`. In this case, you cannot delete the files as a root user. You must log on to the shared file system as a support user.

    ```
    [ root@<svc-hostname> ~]# ssh support@<nas_console>
    ```

6. Search for an export mount point.

   The example below shows how to search for the export mount point. The export is mounted on `<deployment-name>-batch`, where `lms999` is the deployment name on the mount in this example:

   ```
   nas_02:~ # mount | grep batch
   /dev/vx/dsk/sfsdg/lms999-batch on /vx/lms999-batch type vxfs (ro,mntlock=VCS →
   ,cluster,crw,delaylog,largefiles,ioerror=mdisable)
   ```

7. Change directory to the 3GPP export directory and delete the 3GPP export file as displayed:

   ```
   nas_02:~ # cd /vx/lms999-batch/data/export/3gpp_export/
   nas_02:/vx/lms999-batch/data/export/3gpp_export # rm -f 1.xml
   ```

8. Change directory to the dynamic export directory and delete the dynamic export file as displayed:

   ```
   nas_02:~ # cd /vx/lms999-batch/data/export/dynamic_export/
   nas_02:/vx/lms999-batch/data/export/dynamic_export # rm -f 1.txt
   ```

9. Log on to ENM and launch the Command Line Interface.

10. Run the following command to delete the export job for which the file was manually deleted.

    ```
    cmedit export -rm -j <job-id>
    ```

11. Repeat from step 1 until the if the capacity of the `/ericsson/batch/` file system is at less than 80%

Results

Space on the `/ericsson/batch/` file system is made available and the export feature is enabled.

5.22 Elasticsearch Database Administration on Physical Deployments

The Elasticsearch Administration script is available on the Management Server (MS) under `/opt/ericsson/elasticsearch/elasticsearch_admin.py`.

This can be used as a troubleshooting or general information utility.

For example, to check the status of all Elasticsearch indices.

Prerequisites

— Access to the MS.

— Access as the `es_admin` user.

- Log on to the ENM MS (Management Server) and switch user to `es_admin`.

```
[root@ieatlms4906 ~]# su es_admin
```

Note: The only authorized ways for administering or troubleshooting Elasticsearch is by using the Elasticsearch Admin Utility, or using procedures defined therein. Access to the Elasticsearch Indexes via CURL or any other interface is strictly prohibited, and may result in Index Corruption and Data Loss. Usage of other features or methods to run any operations/monitoring or activities on data managed by the Elasticsearch Service is prohibited. If there are any features needed that are not provided and documented herein then contact Ericsson Support.

Post upgrade, the user and group permissions of the export path which are configured during the `Log export configuration` and `Export audit logs options` must be `es_admin:es_admin`.

If in any case permissions for user and group for log export path is not `es_admin:es_admin`. Manual work around is required.

To check the user and group permissions, execute the following command:

```
[root@ieatlms4908 opt]# ls -ld /ericsson/enm/dumps/export_logs_every_5_
minutes_with_retention_1_hours
drwxr-xr-x. 2 es_admin es_admin 8192 Jun 16 14:00 /ericsson/enm/dumps/e
xport_logs_every_5_minutes_with_retention_1_hours
```

To change the user and group permissions to `es_admin:es_admin`, execute the following steps:

1. Log on to the ENM MS as a `root` user.
2. Change permissions to `es_admin:es_admin`:

   ```
   chown -R es_admin:es_admin <absolute export path>
   ```

   For Example:

   ```
   [root@ieatlms4908 opt]# chown -R es_admin:es_admin /ericsson/enm/du
   mps/export_logs_every_5_minutes_with_retention_1_hours
   ```

5.22.1 Elasticsearch Administration

> The `elasticsearch_admin.py` script is executable on the MS and provides an interactive menu for querying Elasticsearch for general information and troubleshooting purposes.

```
[es_admin@ieatlms4906 ~]# python /opt/ericsson/elasticsearch/elasticsearch_admin →
 →
.py
********************************************************************************

ENM - ELASTICSEARCH DBA UTILITY

********************************************************************************

Select the action you want to perform:

0. Quit
1. Version
2. File System
3. Health Check
4. Display Index List
5. Export an Index
6. Run 'remove_err_warn_logs'
7. Manage 'remove_err_warn_logs_cron' Cron Job
8. Terminate 'remove_err_warn_logs_cron.py'
9. Log export configuration(ELECT)
10. Export Audit Logs
11. On demand export of ENM logs

Enter your choice [1-11 or 0 to exit]:
```

The `/opt/ericsson/elasticsearch/elasticsearch_admin.py` script can be executed without the menu, by using the optional parameters set out in Elasticsearch Database Administration Options on page 180.

Selecting option 9 displays the following options:

```
********************************************************************

LOG EXPORT CONFIGURATION(ELECT)

********************************************************************************


Select the option to perform:

0. Previous menu
1. Create new export policy
2. List existing export policies
3. Manage existing export policies

Enter the option to perform:
```

— To create a new export policy, select option 1:

```
********************************************************************************
```

```
CREATE NEW EXPORT POLICY

*************************************************************************

Enter the export path to be stored (leave empty to consider default path /er
icsson/enm/dumps):

Select retention period from below options

1. Set retention period for 1 hour
2. Set retention period for 3 hours
3. Set retention period for 6 hours
4. Set retention period for 12 hours

Select retention period for export files (press enter for default log retent
ion of 12 hours) :
```

Select the frequency period:

```
Set Log Export Frequency

1. Export previous day index
2. Export logs every 6 hours
3. Export logs every hour
4. Export logs every 15 minutes
5. Export logs every 5 minutes

Select the frequency to export log:
```

- Select any of the options to display the following list of filters:

```
Select a parameter to apply filter to export or press enter to continue
with creating policy


You can apply a maximum of two filters to export logs

1. Severity
2. tag
3. hostname
4. program
5. Facility_code
6. Custom_application_logs

Select the filter to apply on export logs:
```

- Selecting option 4, `Program`, displays the following:

  Note: If you enter an incorrect value for the filters program, tag, and hostname then you can use the wildcard option.For example, in the following example the actual value is **JBOSS** but if you entered **JBOSSS**, the script proceeds to use the wildcard. Using this, on entering **JBOS***, all the values that start with JBOS are displayed.

```
Enter value:JBOSSS
Either the value given doesn't have logs or invalid, try using wildcard:
 JBOS*
     1: JBOSS
enter number:1
```

- Entering the value as **JBOSSS** returns a message asking to try using the wildcard **JBOS***. On selecting, option 1: JBOSS from the above displays the following:

```
Select a parameter to apply filter to export or press enter to continue with creating policy

You can apply a maximum of two filters to export logs

     1. Severity
     2. Tag
     3. Hostname
     4. Facility_code
     5. Custom_application_logs

Select the filter to apply on export logs:
```

- Selecting option 1, `Severity`, displays the following:

```
Select severity to filter

1. Error
2. Info
3. Warning
4. Notice
5. Critical
6. Emergency
7. Alert
8. Debug
0. Previous Menu

Select severity:
```

- Selecting option 5, `Critical`, displays the following:

```
Policy created successfully at /opt/ericsson/elasticsearch/policies/export_logs_every_15_minutes_with_retention_1_hours_JBOSS_crit.json

Cron created successfully

Press <RETURN> to continue.
```

Example:

Policy created from previous filter selection:

```
{
"is_enabled": true,
"cron_name": "export_logs_every_6_hours_with_retention_1_hours_JBOSS_crit",
"frequency": [
"0 */06 * * *",
"every 6 hours",
6,
"hours"
],
"wild_card": "program",
"query": {
"program.keyword": "JBOSS",
"severity.keyword": "crit"
},
"export_path": "/ericsson/enm/dumps",
"retention": [
1,
"hours"
]
}
```

Use the `Facility_code`filter to export logs of a specific `facility_code`. Select this filter to get a list of `facility_codes` available for logs in Elasticsearch along with their corresponding facility.

Use the `Custom_application_logs` to export the custom application logs that are sent to Elasticsearch through the `rsyslog conf` files. After you select a `conf` file in by selecting this filter, all the logs that are sent through that `conf` file are exported.

Note:

— After applying the first filter if you want to apply a second filter, the script displays the filter options that are available after the first filter is applied.

If the you select Tag filter with `CROND[<pid>]`, then all the logs with Tag `CROND[pid]` are exported and the policy details are updated as `"wild_card": "CROND$"`. If you do not have the required value of the filter even after display of wildcard, press **i** and give the filter name and the script creates the policy.

If you use a `wild_card`, the script updates the `wild_card` in the policy file with the filter applied, else the policy file is not updated. For example, in the policy file :`"wild_card": "program"`.

If the first filter `Program = neo4j_debug_log` is applied to a policy and you want to apply the Hostname as the second filter for policy creation, then the script displays the possible Hostnames that are available after applying the `Program` filter, as shown in the following example:

```
Select the frequency to export log: 3

Select a parameter to apply filter to export or press ente →
r to continue with creating policy

You can apply a maximum of two filters to export logs

1. Severity
2. Tag
3. Hostname
4. Program
5. Facility_code
6. Custom_application_logs

Select the filter to apply on export logs: 4
Enter value:Neo4j
Either the value given doesn't have logs or invalid, try u →
sing wildcard(Eg-CRON*): neo4*
1: neo4j_txn_log_retention_update 3: neo4j_dps_script_exec →
 5: neo4j_availability_check
2: neo4j_debug_log 4: neo4j_log 6: neo4j_data_monitor
enter number or press i to provide a user defined value:3

Select a parameter to apply filter to export or press ente →
r to continue with creating policy

You can apply a maximum of two filters to export logs

1. Severity
2. Tag
3. Hostname
4. Facility_code
5. Custom_application_logs

Select the filter to apply on export logs:
Select the filter to apply on export logs: 3
1: cloud-db-1
enter number or press i to provide a user defined value:1

Policy created successfully at /opt/ericsson/elasticsearch →
/policies/export_logs_every_hour_with_retention_1_hours_ne →
o4j_dps_script_exec_cloud-db-1.json

Cron created successfully

Press <RETURN> to continue..
```

— Logs exported to export file will be in csv format.

Order of **Headers** for each field in each message in the export file are as follows:

1. severity code

— Selecting option 2 in this sub-menu lists the policies present to export logs:

Note: You can create only two export policies excluding the audit policy. Maximum three policies can be created, one audit policy and two generic policies.

```
*****************************************************************************

LIST EXISTING EXPORT POLICIES

*****************************************************************************



Select the policy option
1. export_logs_every_6_hours_with_retention_1_hours_JBOSS_crit.json
2. export_logs_every_hour_with_retention_1_hours_neo4j_dps_script_exec_cloud →
-db-1.json

Select the option to view current policy details: 1
{
"is_enabled": true,
"disabled_time": "2020-07-28 10:37:47.037259",
"retention": [
1,
"hours"
],
"frequency": [
"0 */06 * * *",
"every 6 hours",
6,
"hours"
],
"wild_card": "program",
"query": {
"program.keyword": "JBOSS",
"severity.keyword": "crit"
},
"export_path": "/ericsson/enm/dumps",
"cron_name": "export_logs_every_6_hours_with_retention_1_hours_JBOSS_crit"
}


Press <RETURN> to continue..
```

Note: The export of logs from the time you disabled can be applied only to export the logs of the current day. It does not include the logs of the previous or any other days before.

— Selecting option 3 displays the following **Enabling a CRON, Disabling a CRON and Removing a CRON:** menu:

```
Select the option to perform:

0. Previous menu
1. Disable existing export policies
2. Enable existing export policies
3. Remove existing export policies

Enter the option to perform:
```

- Selecting option 1 disables the policy to stop exporting logs:

```
Select the policy option
1. export_logs_every_6_hours_with_retention_1_hours_JBOSS_crit.json
2. export_logs_every_hour_with_retention_1_hours_neo4j_dps_script_exec_c →
loud-db-1.json
```

```
Select the option to view current policy details: 1
{
"is_enabled": true,
"disabled_time": "2020-07-28 10:37:47.037259",
"retention": [
1,
"hours"
],
"frequency": [
"0 */06 * * *",
"every 6 hours",
6,
"hours"
],
"wild_card": "program",
"query": {
"program.keyword": "JBOSS",
"severity.keyword": "crit"
},
"export_path": "/ericsson/enm/dumps",
"cron_name": "export_logs_every_6_hours_with_retention_1_hours_JBOSS_cri →
t"
}

Are you sure you want to disable the policy? [Y/n] :y


Selected policy export_logs_every_5_minutes_with_retention_12_hours_JBOS →
S_crit.json disabled successfully


Press <RETURN> to continue..
```

- Selecting option 2 enables the policy to export logs:

```
Select the policy option
1. export_logs_every_5_minutes_with_retention_12_hours_JBOSS_crit.json
2. export_logs_from_previous_day_index_with_retention_12_hours_security. →
json

Select the option to view current policy details:2

{
"is_enabled": false,
"disabled_time": "2020-07-28 10:37:47.037259",
"retention": [
1,
"hours"
],
"frequency": [
"0 */06 * * *",
"every 6 hours",
6,
"hours"
],
"wild_card": "program",
"query": {
"program.keyword": "JBOSS",
"severity.keyword": "crit"
},
"export_path": "/ericsson/enm/dumps",
"cron_name": "export_logs_every_6_hours_with_retention_1_hours_JBOSS_cri →
t"
}

Are you sure you want to re-enable the policy? [Y/n] :y

Do you want export logs from the time you disabled? [Y/n]: y


Selected policy export_logs_every_6_hours_with_retention_1_hours_JBOSS_c →
rit.json enabled successfully


Press <RETURN> to continue..
```

- Selecting option 3 removes the policy to export logs:

```
Enter the option to perform: 3

Select the policy option
1. export_logs_every_6_hours_with_retention_1_hours_JBOSS_crit.json
2. export_logs_every_hour_with_retention_1_hours_neo4j_dps_script_exec_c →
loud-db-1.json

Select the option to view current policy details: 1
{
"is_enabled": true,
"retention": [
1,
"hours"
],
"frequency": [
"0 */06 * * *",
"every 6 hours",
6,
"hours"
],
"wild_card": "program",
"query": {
"program.keyword": "JBOSS",
"severity.keyword": "crit"
},
"cron_name": "export_logs_every_6_hours_with_retention_1_hours_JBOSS_cri →
t",
"export_path": "/ericsson/enm/dumps"
}

Are you sure you want to remove the selected policy ? [Y/n] :y

Cron file removed successfully!

Export policy file removed successfully!


Press <RETURN> to continue..
```

To export Audit logs specifically, select option-10.

Audit logs include the `audit`, `authpriv`, and `syslog` Facility in elasticsearch. You can choose the facility manually. The default facility codes that are exported are; 5, 10, or 13.

You can create only one audit policy at a time. To create a new audit policy, you must delete the existing policy.

You can find the procedure to create an audit log policy from the elasticsearch log admin tool.

Example:

1. In the elasticsearch log admin tool, select option-10:

```
*********************************************************************

EXPORT AUDIT LOGS

*********************************************************************
Select option to perform :

1.Set profile for audit logs
2.Export all security log history stored in Elasticsearch index
3.Export security log history with user defined timestamps
```

```
4.Export security logs for today(Captures all audit logs in current day ES i →
ndex till current time)
```

2. Select the option to perform. Select option 1 and perform the following steps:

   a. Enter the path where you want the log to be exported. The default path is `/ericsson/enm/dumps`.

   b. Select the retention period for the log export files. The default log retention period is 12 hours:

```
************************************************************************ →
****

SET SCHEDULED EXPORT POLICY FOR AUDIT LOG

************************************************************************ →
****



Enter the export path to be stored (leave empty to consider default pat →
h /ericsson/enm/dumps):

Select retention period from below options

1. Set retention period for 1 hour
2. Set retention period for 3 hours
3. Set retention period for 6 hours
4. Set retention period for 12 hours

Select retention period for export files (press enter for default log r →
etention of 12 hours) :
```

   c. Select the frequency to export logs:

```
Set Log Export Frequency

1. Export previous day index
2. Export logs every 6 hours
3. Export logs every hour
4. Export logs every 15 minutes
5. Export logs every 5 minutes

Select the frequency to export log: 5
```

   d. Policy is created successfully. Press **Return** to continue.

```
Policy created successfully at /opt/ericsson/elasticsearch/policies/exp →
ort_logs_every_5_minutes_with_retention_6_hours_security.json

Cron created successfully


Press <RETURN> to continue.
```

3. Select option 2 to export all security logs from the previous elasticsearch indexes:

```
************************************************************************

EXPORT HISTORICAL AUDIT LOGS RESIDING ON THE DEPLOYMENT

************************************************************************
```

```
Select elasticsearch index from below options :

1. enm_logs-application-2020.07.27
2. enm_logs-application-2020.07.23
3. enm_logs-application-2020.07.24
4. enm_logs-application-2020.07.26

Select index for filtering audit logs : 2

Selected elasticsearch index : enm_logs-application-2020.07.23

Enter export_path (Press enter to consider default path as /ericsson/enm/dum
ps):

By default facility code 5, 10, 13 logs will be fetched. Do you want to proc
eed press enter else provide facility codes seperated by (,):

Provide Username to filter audit logs by (press return for none):


Processing request...

Exporting audit logs from enm_logs-application-2020.07.23 index to /ericsson
/enm/dumps/export_all_security_logs_in_selected_index/2020-07-28-09-59-25.cs
v.gz

Fetch completed for audit policy...!


Press <RETURN> to continue..
```

4. Select option 3 to export security logs with specific timestamps:

```
************************************************************
**************

EXPORT AUDIT LOG HISTORY OF EACH DAY IN SEPARATE FILES

************************************************************
**************



Select elasticsearch index from below options :

1. enm_logs-application-2020.07.28
2. enm_logs-application-2020.07.27
3. enm_logs-application-2020.07.23
4. enm_logs-application-2020.07.24
5. enm_logs-application-2020.07.26

Select index for filtering audit logs : 2

Selected elasticsearch index : enm_logs-application-2020.07.2
7

Enter start time of capture (Example format : 05:15:01) : 05:
01:12

Enter end time of capture (Example format : 10:15:01) : 15:01
```

```
:05

Enter export_path (Press enter to consider default path as /e →
ricsson/enm/dumps):

By default facility code 5, 10, 13 logs will be fetched. Do y →
ou want to proceed press enter else provide facility codes se →
perated by (,):

Provide Username to filter audit logs by (press return for no →
ne):



Processing request...

Exporting audit logs from enm_logs-application-2020.07.27 ind →
ex to /ericsson/enm/dumps/export_security_logs_for_defined_ti →
mestamps/2020-07-28-09-59-25.csv.gz

Fetch completed for audit policy...!


Press <RETURN> to continue..
```

5. Select option 4 to export security logs from the current ES till the current time:

```
*********************************************************************

EXPORT AUDIT LOGS FOR TODAY

*********************************************************************


Enter export_path (Press enter to consider default path as /ericsson/enm/dum →
ps):

By default facility code 5, 10, 13 logs will be fetched. Do you want to proc →
eed press enter else provide facility codes seperated by (,):

Provide Username to filter audit logs by (press return for none):

Processing request...

Exporting audit logs from enm_logs-application-2020.07.28 index to /ericsson →
/enm/dumps/export_current_day_security_logs/2020-07-28-11-04-58.csv.gz

Fetch completed for audit policy...!


Press <RETURN> to continue..
```

6. Select option 11 from Elasticsearch DBA tool menu to capture and export ENM logs at one off. Use this feature to:

   - Export ENM logs on demand.

- Export historical data of the logs in the elasticsearch index from last 1 minute, last 5 minutes, last 15 minutes, last 1 hour, last 3 hours, current day, and previous day.
- Capture and export filtered ENM logs using the filtering options provided.

After you select all the options, the log file is generated at the selected export path.

Example:

```
*********************************************************************

ON DEMAND EXPORT OF ENM LOGS

*********************************************************************



Enter the path for exported logs to be stored (leave empty to consider defau →
lt path /ericsson/enm/dumps):

Select export timeline from below options

1. Export historical data from older ES indices
2. Export current day's data
3. Export last 3 hours data
4. Export last 1 hour data
5. Export last 15 minutes data
6. Export last 5 minutes data
7. Export last 1 minute data

Select export timeline: 5

Select a parameter to apply filter to export or press enter to continue with →
 creating policy

You can apply a maximum of two filters to export logs

1. Severity
2. Tag
3. Hostname
4. Program
5. Facility_code
6. Custom_application_logs

Select the filter to apply on export logs: 1

Select severity to filter

1. Error
2. Info
3. Warning
4. Notice
5. Critical
6. Emergency
7. Alert
8. Debug
0. Previous Menu

Select severity : 2

Select a parameter to apply filter to export or press enter to continue with →
 creating policy

You can apply a maximum of two filters to export logs

1. Tag
2. Hostname
3. Program
4. Facility_code
5. Custom_application_logs
```

```
Select the filter to apply on export logs:

Processing Request...

Fetching data...

Fetch completed.

Log File path : /ericsson/enm/dumps/enm-csv-logfile-having_last-15minutes-da →
ta_2020-07-15_07-32.gz


Press <RETURN> to continue..
```

5.22.2 Export of Logs with es_admin as a User

To pull out the exported logs from the export path using scp/sftp into an external server:

```
[root@ieatlms4419 export]# scp -r es_admin@ieatlms4906:/ericsson/enm/dumps/expor →
t* .
The authenticity of host 'ieatlms4906 (141.137.250.251)' can't be established.
RSA key fingerprint is 38:11:08:38:3e:c5:85:47:d2:36:63:22:71:3a:ee:7c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ieatlms4906,141.137.250.251' (RSA) to the list of kn →
own hosts.
############ WARNING ############

This system is for authorised use only. By using this system you consent to moni →
toring and data collection.

#################################
es_admin@ieatlms4906's password:
enm-csv-logfile-2020-04-15-04-15-01.gz 100% 287KB 287.2KB/s 00:00
enm-csv-logfile-2020-04-15-04-15-01.gz 100% 16KB 15.6KB/s 00:00
```

5.22.3 Elasticsearch Database Administration Options

Option	Description
1) Version	Displays the version of Elasticsearch installed.
2) File System	Displays a summary of Elasticsearch file system information.
3) Health Check	Health status on the health of the cluster.
4) Display Index List	Displays a list of all Elasticsearch indexes along with their size and status.
5) Export an Index	Export the logs of an Elasticsearch index to a `.gz` file in a specified location. Option 4 displays the Elasticsearch indexes size. Ensure that the specified location has enough space.
6) Run 'remove_err_warn_logs'	Removes all `err` and `warning` logs of facility local5 greater than seven days old.
7) Manage 'remove_err_warn_logs_cron' Cron Job	Enable or disable the crontab entry `/etc/cron.d/remove_err_warn_logs_cron`.
8) Terminate 'remove_err_warn_logs_cron.py'	If an instance of the `remove_err_warn_logs.py` script is running, this instance of the script is ended. If enabled, the `remove_err_warn_logs.py` is activated in the next crontab. This is, by default, at 1 am the next day. **Note:** This option must be executed before performing an Upgrade.

Option	Description
9) Log export configuration(ELECT)	By running this option, any of the options displayed can be selected that are performed on the data export: 1. `Create export policy.` By selecting this option, the policy file is created as per user selected frequency. Using this policy file, cron performs time-based export of elasticsearch logs in external export path that is mounted to db node. — `Buffer time of 1 minute is maintained to make sure no data is lost.` Example for 5 minutes policy (executed every 0, 5, 10, 15, and so on). If policy is created at 10:18 PM, cron executes at 10:20 PM. In export file, logs are collected starting from 10:14 PM, and last log collected is at 10:19 PM (5 minutes time delta). Buffer time of 1 minute is maintained to allow for writing of logs to elasticsearch. Logs at 10:20 PM are not captured. — `Limitation: Data duplication can occur for 1 minute.` Data may be duplicated for 1 minute, depending on accuracy of cron execution. Example for 5 minutes policy, if cron first executes at 10:20:01 PM, and executes again at 10:25:01 PM, the logs are duplicated at 10:19 PM (logs captured from 10:19 PM to 10:24 PM). 2. `List existing export policies.` By selecting this option, the list of all the created policies is displayed. 3. `Manage export policies.` By selecting this option, the user can Enable, Disable, or Remove a existing cron.
10) Export Audit logs	Execute this option to display the following options that you can select to perform data export. 1. Set profile for security logs This option creates the policy file per the selected frequency. Using this policy file, cron performs a time based export of elasticsearch security logs to an external export path that is mounted on the db node. 2. Export all security log history stored in Elasticsearch index This option exports security logs for the selected elasticsearch index as per user selected facility codes (5, 10, 13). 3. Export security log history with user defined timestamps This option exports the security logs for the selected elastic search index as per user defined time stamps and facility codes. 4. Export security logs for today(Captures all audit logs in current day ES index till current time) This option exports all the security logs for the present day elastic search index as per the user selected facility code.
11) On demand export of ENM logs	Use this option to: — Capture and export ENM logs at one off as per the selected frequency. — Capture and export ENM logs in elasticsearch indices history. You can also use the filtering options that are provided to capture and export the filtered logs.

The `/opt/ericsson/elasticsearch/elasticsearch_admin.py` script can be executed without the menu by using the following optional parameters:

```
[es_admin@ieatlms4906 elasticsearch]$ ./elasticsearch_admin.py -h
usage: elasticsearch_admin.py menu [-h] [-v] [-f] [-hc] [-l] [-e] [-r] [-c]
[-dis] [-el] [-a] [-o]

optional arguments:
```

```
-h, --help show this help message and exit
-v, --version Elasticsearch Version
-f, --filesystem Elasticsearch File System Info
-hc, --healthcheck Elasticsearch Health Check
-l, --list Display Elasticsearch indices
-e, --export Export Elasticsearch logs
-r, --remove Elasticsearch Delete Error and Warning logs
-c, --cron Elasticsearch Manage Cron Job
-dis, --disable Terminate 'remove_err_warn_logs.py'
-el, --elect Elasticsearch Log Export Configurable Tool
-a, --audit audit_logs
-o, --on_demand One off data export with filtering options
```

```
-elect-audit-policy [-h] --path PATH --log-retention {12 hours,6 hours,3 hours,1 →
 hour}--frequency{previous day index,every 6 hours,every 1 hour,every 5 minutes, →
every minute} , Creates audit policy

Example:

# python elasticsearch_admin.py elect-audit-policy --path "/ericsson/enm/dumps"  →
--log-retention "12 hours" --frequency "every 6 hours"

Policy created successfully at /opt/ericsson/elasticsearch/policies/export_logs_ →
every_6_hours_with_retention_12_hours_audit.json
```

```
-elect-create-policy [-h] --path PATH --log-retention {12 hours,6 hours,3 hours, →
1 hour} --frequency {previous day index,every 6 hours,every 1 hour,every 5 minut →
es,every minute} [--filters FILTERS] , - creates new policy.

Example :

# python elasticsearch_admin.py elect-create-policy --path "/ericsson/enm/dumps" →
 --log-retention "1 hour" --frequency "every 6 hours" --filters '{"severity":"in →
fo"}'

Policy created successfully at /opt/ericsson/elasticsearch/policies/export_logs_ →
every_6_hours_with_retention_1_hours_info.json
```

```
-elect-list-policies , - lists all available policies

Example :

# python elasticsearch_admin.py elect-list-policies
```

```
-elect-manage-policies [-h] [--disable-policy DISABLE_POLICY][--enable-policy EN →
ABLE_POLICY][--remove-policy REMOVE_POLICY], - Manage policies like remove or en →
able or disable policies

Example:

# python elasticsearch_admin.py elect-manage-policies --enable-policy export_log →
s_every_6_hours_with_retention_1_hours_neo4j.json

Selected policy export_logs_every_6_hours_with_retention_1_hours_neo4j enabled s →
uccessfully

# python elasticsearch_admin.py elect-manage-policies --disable-policy export_lo →
gs_every_6_hours_with_retention_1_hours_neo4j.json

Selected policy export_logs_every_6_hours_with_retention_1_hours_neo4j disabled  →
successfully

# python elasticsearch_admin.py elect-manage-policies --remove-policy export_log →
s_every_6_hours_with_retention_1_hours_neo4j.json
```

Following is the argument parser for option 11 in the Elasticsearch DBA tool menu:

```
[es_admin@ieatlms4906 elasticsearch]$ ./elasticsearch_admin.py export-logs-in-on →
e-off --help
usage: elasticsearch_admin.py export-logs-in-one-off [-h] --path PATH
--frequency
{current-days-data,last-3-hours-data,last-1-hour-data,last-15-minutes-data,last- →
5-minutes-data,last-1-minute-data}
[--filters FILTERS]

optional arguments:
-h, --help show this help message and exit
--path PATH Path to export logs
--frequency {current-days-data,last-3-hours-data,last-1-hour-data,last-15-minute →
s-data,last-5-minutes-data,last-1-minute-data}
Capture data of following from index and export
--filters FILTERS Available filters 1.tag 2.severity 3.host 4.program
example:'{"severity":"info"}'

Example :

./elasticsearch_admin.py export-logs-in-one-off --path '/ericsson/enm/dumps' --f →
requency last-5-minutes-data --filters '{"severity":"info"}'

To export logs from history indices :

[es_admin@ieatlms4906 elasticsearch]$ ./elasticsearch_admin.py export-log-histor →
y-in-one-off --help
usage: elasticsearch_admin.py export-log-history-in-one-off
[-h] --index INDEX --path PATH [--filters FILTERS]

optional arguments:
-h, --help show this help message and exit
--index INDEX export data from given index
--path PATH Path to export logs
--filters FILTERS Available filters 1.tag 2.severity 3.host 4.program
example:'{"severity":"info"}'

Example :

./elasticsearch_admin.py export-log-history-in-one-off --index 'enm_logs-applica →
tion-2020.07.10' --path '/ericsson/enm/dumps' --filters '{"severity":"info"}'
```

5.22.4 Change the Elasticsearch Retention Period

The default retention period for Elasticsearch is 7 days. This task describes how to customize the retention period. You may want to reduce the retention period due to insufficient disk space, or extend the period to have access to older logs.

Prerequisites

- You have root access to the management server.
- ElasticSearch is in a consistent and working state.
  - You can see log entries in Elasticsearch.
- There are no unapplied changes in the LITP model.

Note: This procedure will not persist an upgrade.

Steps

1. Check the existing retention period value in the LITP model.

Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.

Run the following command:

```
[root@ms-1]# litp show -p /software/services/elasticsearch/
```

You can see a property called `log_retention_in_days`. The value for this is the current retention period.

```
...
        service_name: elasticsearch
        max_log_data_in_gb: 480.0
        log_retention_in_days: 7
        index_number_of_replicas: 1
        discovery_zen_ping_multicast_enabled: false
...
```

2. Modify the LITP model with the desired value.

   Run the following command, replacing `NEW_RETENTION` with your desired new retention period.

```
[root@ms-1~]# litp update -p /software/services/elasticsearch/ -o log_retent →
ion_in_days=NEW_RETENTION
```

3. Check that the new value is in the LITP model.

```
[root@ms-1]# litp show -p /software/services/elasticsearch/ -o log_retention →
_in_days
```

4. Create a new LITP plan for the changes.

```
[root@ms-1~]# litp create_plan
```

   Note: Any other unapplied LITP model changes are included in this plan.

5. Run the newly created LITP plan.

```
[root@ms-1~]# litp run_plan
```

6. Monitor the execution of the LITP plan.

   This can be done using the following command:

```
[root@ms-1~]# watch litp show_plan -a
```

7. Clean the logs from ElasticSearch.

   When the LITP plan shows that all tasks have executed successfully and if the retention period has been decreased (for example from 7 days to 3 days), the logs from before the new retention period must be cleaned from

ElasticSearch or they will still exist. You can run this operation manually using the following command from the db node.

```
[root@ms-1~]# ssh litp-admin@<db hostname>
[root@db-1~]# /etc/cron.daily/clean_elasticsearch
```

Note: Logs of severity *<err>* and *<warning>* and of facility *<local5>* that are older than 7 days are removed

5.22.5 Elasticsearch Log Retention Size Limit

This task describes how to customize the logs retention size limit. It may be necessary to reduce the log retention size due to insufficient disk space, or extend the size to keep more logs.

Prerequisites

- You have root access to the management server.
- ElasticSearch is in a consistent and working state.
  - You can see log entries in Elasticsearch.
- There are no unapplied changes in the LITP model.

Steps

1. Check the existing retention storage size value in the LITP model

   Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.

   Run the following command:

   ```
   [root@ms-1]# litp show -p /software/services/elasticsearch/
   ```

   Verify value of property `max_log_data_in_gb`. The value for this is the current retention storage size.

   ```
   ...
           path_conf: /etc/elasticsearch
           service_name: elasticsearch
           max_log_data_in_gb: 480.0
           log_retention_in_days: 7
           index_number_of_replicas: 1
   ...
   ```

   a. Modify the LITP model with the desired value.

      Run the following command, replacing `NEW_RETENTION_SIZE` with your desired new retention storage size.

```
[root@ms-1~]# litp update -p /software/services/elasticsearch/ -o m →
ax_log_data_in_gb=NEW_RETENTION_SIZE
```

2. Check that the new value is in the LITP model

```
[root@ms-1]# litp show -p /software/services/elasticsearch/ -o max_log_data_ →
in_gb
```

3. Create a new LITP plan for the changes

```
[root@ms-1~]# litp create_plan
```

Note: Any other unapplied LITP model changes are included in this plan.

4. Run the newly created LITP plan

```
[root@ms-1~]# litp run_plan
```

5. Monitor the execution of the LITP plan

   This can be done using the following command:

```
[root@ms-1~]# watch litp show_plan -a
```

6. Clean the logs from ElasticSearch

   When the LITP plan shows that all tasks have executed successfully and if the retention size is reduced, the logs from before the new retention period should be cleaned from ElasticSearch. The oldest index of ElasticSearch is deleted by the day until the size of logs is less than the maximum retention size. This operation runs automatically every hour, or can be run manually using the following command from the db node:

```
[root@ms-1~]# ssh litp-admin@<db hostname>
[root@db-1~]# /etc/cron.hourly/clean_elasticsearch_hourly
```

Results

The retention storage size limit is changed and logs outside of the new size limit are deleted on a "by day" basis, beginning from the oldest day.

5.23 Check the OpenAM DB Size in Physical ENM

This topic describes how to check the size of the Open Access Management (OpenAM) database (DB) size. If the value of the OpenAM DB is greater than 150000 entries, then you must apply the corrective actions outlined in this topic in order to avoid a cleanstart of the Single Sign On (SSO) services.

Prerequisites

— You have `root` and `litp-admin` user access to the SVC nodes.

— You have `root` user access to the Management Server (MS).

Steps

1. Log on to the ENM MS as the litp-admin user and switch to the root user.
2. Determine the SSO VM instances applicable for your deployment.

   ```
   [root@ms-1 ~]# cat /etc/hosts | grep sso | grep svc-
   ```

   Example

   ```
   10.247.246.129 svc-2-sso sso-2-internal # Created by LITP. Please do not edi →
   t
   10.247.246.128 svc-1-sso sso-1-internal # Created by LITP. Please do not edi →
   t
   ```

3. For each of the SSO VM's perform the following actions:

   a. Log on to the SSO VM from the MS:

      ```
      [root@ms-1 ~]# ssh -i /root/.ssh/vm_private_key cloud-user@svc-1-ss →
      o
      Last login: Tue Sep 19 15:48:24 2017 from ms-1
      [cloud-user@svc-1-sso ~]$ sudo su -
      [root@svc-1-sso ~]#
      ```

   b. Check the number of OpenAM DB entries. Ensure that you enter the following as a single line command:

      ```
      [root@svc-1-sso]# /opt/ericsson/sso/heimdallr/opends/bin/ldapsearch →
       --port 10389 --bindDN "cn=Directory Manager" -w `cat /opt/ericsson →
      /sso/config/config-access.bin` --baseDN "cn=monitor" --searchScope →
      sub "(cn=userRoot backend)" | grep "ds-backend-entry-count:"
      ```

      The expected result is similar to the following:

      ```
      ds-backend-entry-count: 6080
      ```

      If the number of OpenAM DB entries is less than `150000` for every SSO VM, then you may skip the remaining steps of this topic.

      If the number of OpenAM DB entries is greater than `150000` for any of the SSO VMs, then you must continue with the corrective actions outlined in the next steps.

4. From the MS, log on to one of the SVC nodes hosting the SSO VM as the `litp-admin` user and then switch to the `root` user.

```
[root@ms-1 ~]# ssh litp-admin@svc-1
litp-admin@svc-1 's password:
[litp-admin@svc-1 ~]$ su -
Password:
[root@svc-1 ~]#
```

5. Power off the SSO service groups by executing the following command. This takes effect on all SSO service instances simultaneously and must be executed only on one SVC host.

```
[root @svc-1 ~]# hagrp -offline Grp_CS_svc_cluster_sso -any
```

Example

```
[root@svc-1 ~]# hagrp -offline Grp_CS_svc_cluster_sso -any
VCS NOTICE V- 16 - 1 - 50733 Attempting to offline group on system svc-1
VCS NOTICE V- 16 - 1 - 50733 Attempting to offline group on system svc-1
[root@svc-1 ~]#
```

6. Verify that the SSO service groups are `OFFLINE` by reviewing the output of the following command:

```
[root@svc-1 ~]# hagrp -state | grep sso
```

Example

```
[root@svc-1 ~]# hagrp -state | grep sso
Grp_CS_svc_cluster_sso              State                 svc-1 |ONLINE|STOP →
PING|
Grp_CS_svc_cluster_sso              State                 svc-2 |ONLINE|STOP →
PING|
[root@svc-1  ~]# hagrp -state | grep sso
Grp_CS_svc_cluster_sso              State               svc-1 |OFFLINE|
Grp_CS_svc_cluster_sso              State               svc-2 |OFFLINE|
```

7. For each SVC node identified in Step 1, execute the following commands:

    a. Log on to the SVC node as the `litp-admin` user and then switch to the `root` user.

    b. Undefine the SSO VM by executing the following command:

    ```
    [root@svc-2 ~]#virsh undefine sso
    ```

    c. Check that the SSO VM has been removed by executing the following command:

    ```
    [root@svc-2 ~]#virsh list --all | grep sso
    ```

    If the VM has been correctly undefined, no output is displayed after running this command.

8. Power on the SSO service groups by executing the following command. This takes effect on all SSO services simultaneously and must be executed only on one SVC host.

```
[root@svc-2 ~]#hagrp -online Grp_CS_svc_cluster_sso -any
```

9. Verify that the service group has fully come ONLINE by reviewing the output of the following command:

```
[root@svc-1 ~]# hagrp -state | grep sso
```

Example

```
[root@svc-2 ~]# hagrp -state | grep sso
Grp_CS_svc_cluster_sso              State                svc-2 |OFFLINE|STAR →
TING|
Grp_CS_svc_cluster_sso              State                svc-1 |OFFLINE|STAR →
TING|
[root@svc-2 ~]# hagrp -state | grep sso
Grp_CS_svc_cluster_sso              State                svc-2 |ONLINE|
Grp_CS_svc_cluster_sso              State                svc-1 |ONLINE|
```

Results

You have verified that the number of OpenAM DB entries is less than 150000.

6 System Level Maintenance Tasks for Openstack Based Deployments

6.1 Shut Down ENM on Cloud

This section describes how to shut down ENM on Cloud using either the manage_enm script or the Cloud Management Workflows.

The key difference between the two is that the manage_enm script shuts down both ENM on Cloud and VNF-LCM VMs, while the Cloud Management Workflows only shut down ENM on Cloud.

The workflow that shuts down ENM on Cloud is **Manage ENM - Shutdown**, which performs either a graceful or hard shutdown of ENM on Cloud.

The graceful option shuts down VMs before deleting stacks, while the hard shutdown deletes stacks without shutting down VMs beforehand. Volumes are retained in both cases.

Prerequisites:

— ENM on Cloud deployed.

— VNF-LCM deployed.

— ERICenmcloudmgmtworkflows_CXP9036442 RPM is installed on VNF-LCM.

— ERICenmdeploymentworkflows_CXP9034151 RPM installed on VNF-LCM.

— VNF-LCM SED is available.

6.1.1 Shut Down ENM on Cloud Using the manage_enm Script

This section describes how to shut down ENM on Cloud and the VNF-LCM VMs. The shutdown procedure changes the state of the VNF-LCM VMs from ACTIVE to SHUTOFF.

The manage_enm script shuts down VNF-LCM VMs by default. Optionally, this step can be excluded.

The manage_enm script performs either a graceful or a hard shutdown of ENM on Cloud.

Note: The VM or external server hosting the ENM cloud management utils RPM is referred to as the ENM cloud management host.

If the manage_enm script is installed on a Linux distribution that is not based on rpm, it will not be available in the system PATH. Therefore, a full path to the executable must be specified when invoking the script, as shown below:

```
$ <extracted_rpm_directory>/bin/manage_enm stop -h
```

Note: Parameter <external_ip_for_services_vm> used in the procedure signifies the VNF-LCM external IP address and corresponds to one of the following values:

- On VNF-LCM High Availability (HA) deployments:

  The <external_ipv4_vip_for_services> or <external_ipv6_for_services> parameter in the VNF-LCM SED.

- On non-HA VNF-LCM deployments:

  The <external_ipv4_for_services_vm> or <external_ipv6_for_services_vm> parameter in the VNF-LCM SED.

The script takes approximately 10 minutes to finish executing with the graceful option and 5 minutes with the hard option.

Prerequisites

- ERICenmcloudmgmtutils_CXP9036444 RPM installed on the ENM cloud management host, as described in *Install ENM Cloud Management RPM* in *ENM on Cloud Deployment Instructions* (Available from local Ericsson Support).
- ENM cloud management host can access VNF-LCM's external network.

  Note: For instructions on how to manage access to VNF-LCM, see *VNF-LCM Admin CLI (VNF-LCM Security Utility subsection)* in the ENM Configuration System Administrator Guide [21].

- OpenStack RC file for the ENM deployment is available on the ENM cloud management host.

Steps

1. Log onto the ENM cloud management host.
2. Source the OpenStack RC file for the ENM deployment.

```
$ source <path_to_RC_file>/<name_of_RC_file>.rc
```

Example:

```
$ source /home/enm-admin/enm_deployment.rc
```

3. Display the help message for the script's stop action.

```
$ manage_enm stop -h
```

Example:

```
$ manage_enm stop -h
INFO: Logging to /root/manage_enm.log
usage: manage_enm.py stop [-h] [--rcfile RCFILE] [--lcm HOST]
[--lcm-name LCM_NAME] [--lcm-db-name LCM_DB_NAME]
[--hard] [--reason REASON] [--skiplcm] [--yes]
optional arguments:
  -h, --help            show this help message and exit
  --rcfile RCFILE       path to the OpenStack RC file
  --lcm HOST            hostname or IP of VNF-LCM workflow service
  --lcm-name LCM_NAME   Custom value for VNF-LCM services server as defined →
in
                        VNF-LCM SED.
  --lcm-db-name LCM_DB_NAME
                        Custom value for VNF-LCM DB server as defined in VNF →
-
                        LCM SED.
  --hard                perform a hard shutdown of ENM
  --reason REASON       reason for shutdown of ENM
  --skiplcm             leave VNF-LCM servers running
  --yes                 skip user prompt before ENM shutdown
```

Note: If called without the --yes flag, the script prompts for confirmation before shutting down ENM on Cloud and VNF-LCM VMs. Answer **YeS** (case sensitive) to proceed with the shutdown.

If the properties <Services_vm_HostName> and <DB_vm_HostName> in the VNF-LCM SED are customized, provide the customized values by using --lcm-name and --lcm-db-name arguments.

4. Shut down ENM and/or VNF-LCM with the graceful (default) or hard option.

   a. Shut down ENM and VNF-LCM VMs gracefully (default).

   ```
   $ manage_enm stop --lcm <external_ip_for_services_vm>
   ```

   b. Shut down ENM and VNF-LCM VMs with the --hard option.

   ```
   $ manage_enm stop --hard --lcm <external_ip_for_services_vm>
   ```

   Example:

   ```
   [enm-admin@manage-enm-server ~]$ manage_enm stop --lcm 10.2.2.1
   INFO: Logging to /home/enm-admin/manage_enm.log

   This procedure will shut down ENM, causing unavailability of servic →
   es. Type "YeS" when you are ready to proceed:  YeS
   INFO: Authenticating with OpenStack
   INFO: Checking if essential OpenStack services are up
   ```

```
INFO: Checking if VNF-LCM workflows are available at "10.2.2.1"
INFO: Stopping ENM with graceful option. Reason: manage_enm - Shutd →
own ENM for planned maintenance
INFO: Starting ShutdownENM__top workflow
INFO: Monitoring workflow instance ShutdownENM_20180716_120327
..............
INFO: Workflow no longer running
INFO: Workflow instance completed successfully
INFO: Stopping VNF-LCM servers
INFO: VNF-LCM servers stopped
[enm-admin@manage-enm-server ~]$
```

Note: If you do not want to shut down VNF-LCM VMs, invoke the script with the --skiplcm option.

If the script fails, do not proceed to the next step, collect the `manage_enm.log` file located under the user home directory and contact Ericsson Support.

5. Follow this step if the script fails due to a connection error like in the example below.

```
INFO: Monitoring workflow instance ShutdownENM_20190206_100741
.....ConnectionError - HTTPConnectionPool(host='vnflaf-services', port=80):  →
Max retries exceeded with url: /wfs/rest/progresssummaries/0b99cb94-29f7-11e →
9-9f71-fa163e760ba7 (Caused by
NewConnectionError('<requests.packages.urllib3.connection.HTTPConnection obj →
ect at 0x7f26a94ac090>: Failed to establish a new connection: [Errno 113] No →
 route to host',))
```

   a. Using the following URL, open the VNF-LCM UI in the browser :

      http://<external_ip_for_services_vm>/index.html#workflows

   b. Click the **Manage ENM - Shutdown** workflow under **Workflows**. The latest workflows are displayed under **Instance Activity**.

   c. Confirm that the most recent **Manage ENM - Shutdown** workflow has completed.

   d. If the most recent workflow has not completed, click on it to view workflow's progress. Click the **Refresh** button in the top right hand corner, to refresh the page and monitor the progress until the workflow is complete.

   e. Re-run the `manage_enm` script with the `stop` action to ensure that the VNF-LCM VMs have been shutdown.

6.1.2 Shut Down ENM on Cloud using Cloud Management Workflows

Prerequisites

VNF-LCM UI is available.

Note: Do not run this procedure when performing the steps mentioned in the *ENM Software Upgrade Pre-Steps* and the *ENM Software Upgrade* chapters of the ENM on Cloud Upgrade Instructions document as unexpected errors can occur.

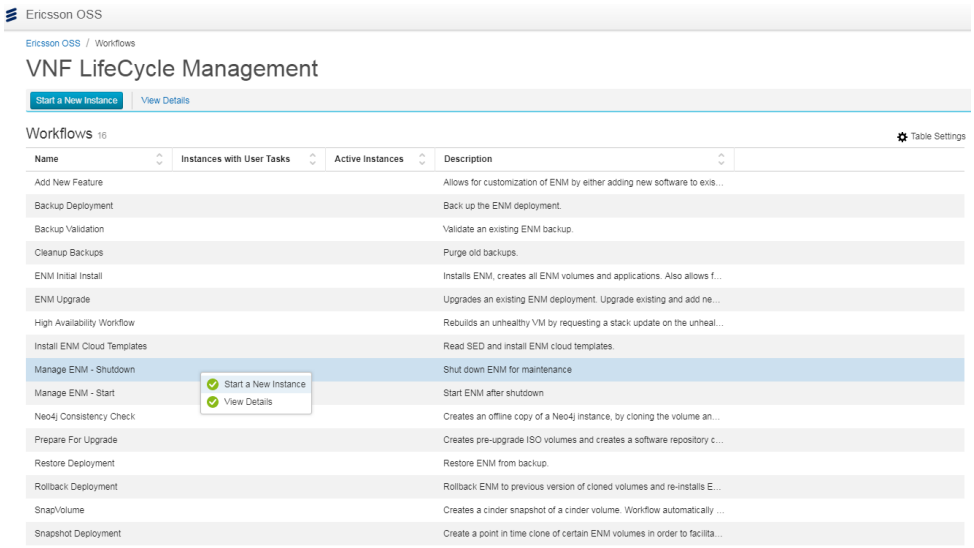
Steps

1. Open the VNF-LCM UI in the browser, using the following URL:

   Note: Replace the value <external_ip_for_services_vm> in the URL with the value corresponding to either the <external_ipv4_vip_for_services> if VNF-LCM deployed in HA Mode or <external_ipv4_for_services_vm> or <external_ipv6_for_services_vm> if VNF-LCM deployed in Non-HA Mode as found on VNF-LCM SED.

   ```
   http://<external_ip_for_services_vm>/index.html#workflows
   ```

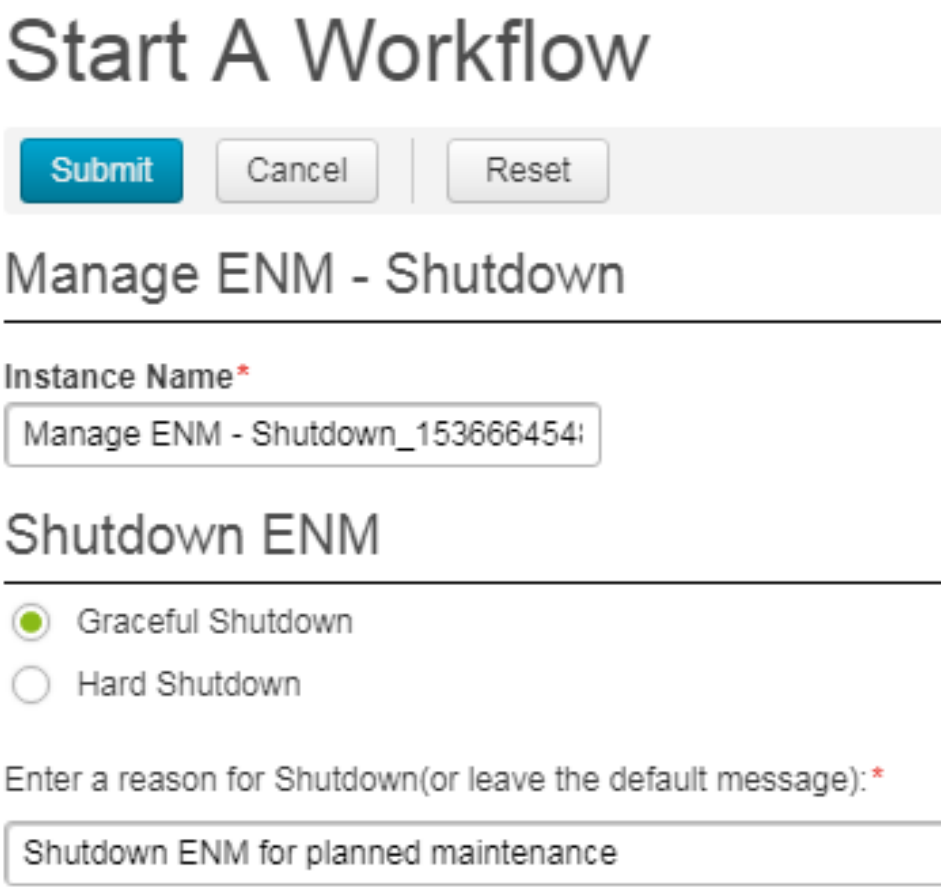
2. Select the **Manage ENM - Shutdown** workflow, then click **Start a New Instance**. Alternatively, right click **Manage ENM - Shutdown** workflow and select **Start a New Instance**.



3. Select either **Graceful Shutdown** or **Hard Shutdown**, then click **Submit** to start the ENM on Cloud shutdown.

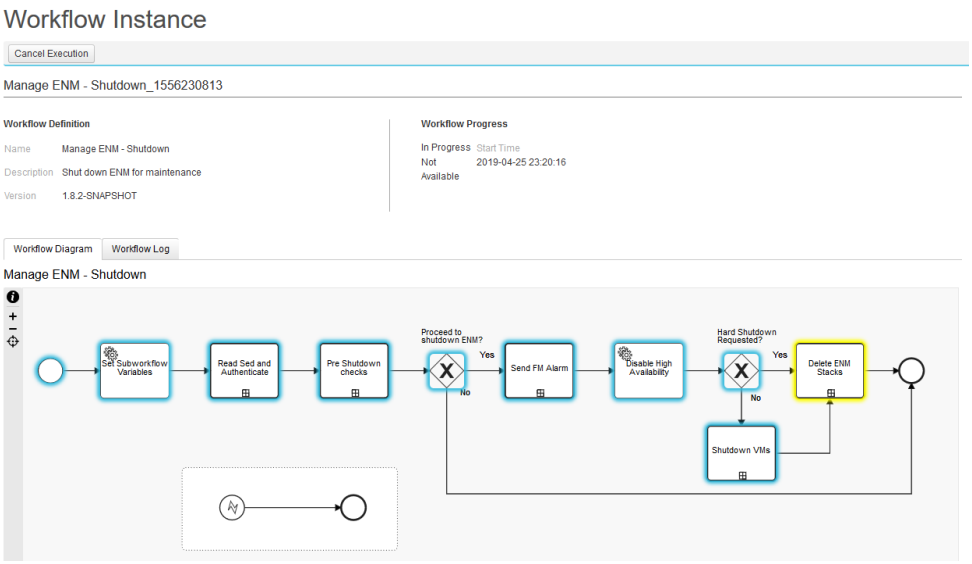
   Example

   A graceful **Manage ENM - Shutdown.**



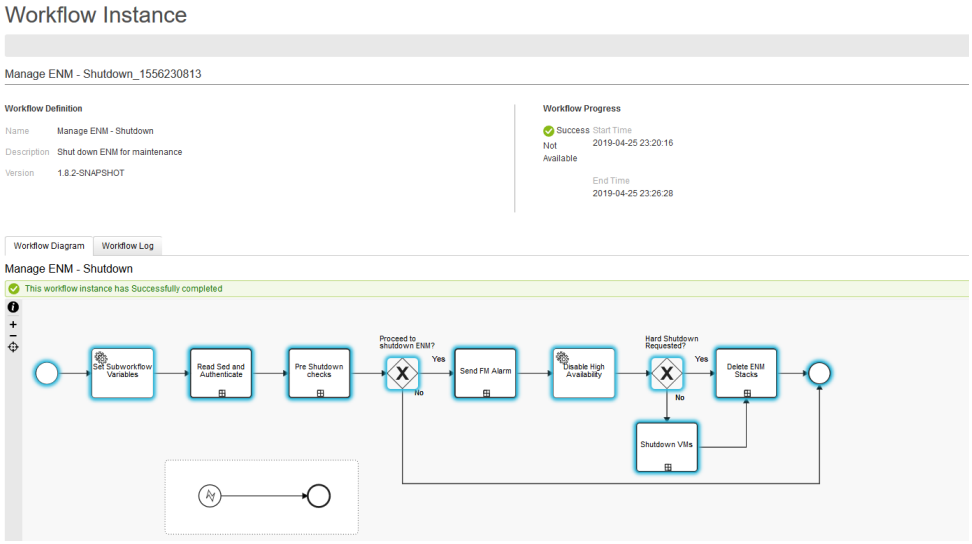
Note: The shutdown reason field can be edited to provide a more detailed reason for the shutdown. This value will be used by the FM alarm in the "Probable Cause" field.

4. Monitor the **Manage ENM - Shutdown** workflow. Use the refresh option to reload and check the progress of the workflow instance.

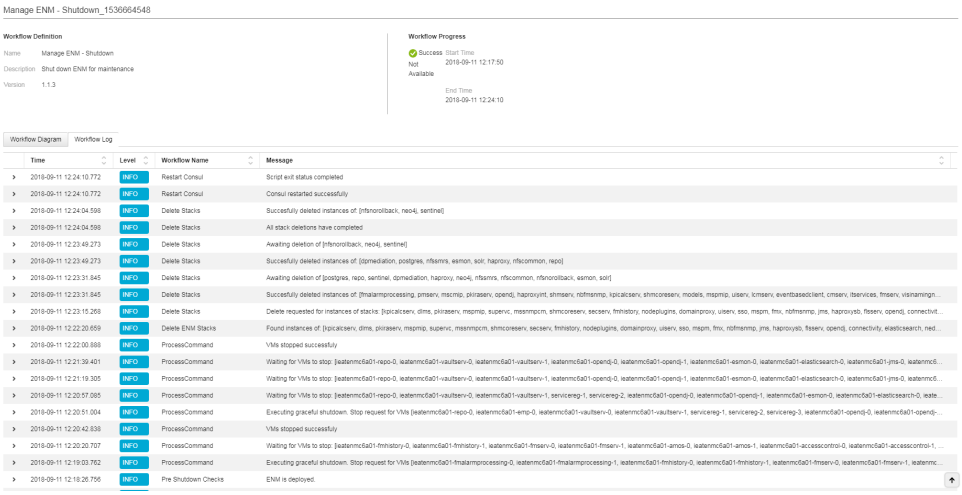


5. Wait for the completion of the **Manage ENM - Shutdown** Workflow.

   Workflow Instance:



   Workflow Log:



6. Gather information about the state of the system after the shutdown:

    a. From an OpenStack client machine source the OpenStack RC file for the ENM on Cloud deployment:

    ```
    # source <OpenStack RC file name>.rc
    ```

    b. Execute the following OpenStack commands to verify the deployment's state:

    ```
    # openstack stack list
     # openstack server list
     # openstack volume list
    ```

    There should be no ENM on Cloud stacks or VMs, only volumes. The VNF-LAF services and database VMs, stacks and volumes should still be present.

    Example

    ```
    [root@vms ~]# openstack stack list --short

    +--------------------------------------+--------------------------
    -----+-----------------+
    | ID                                   | Stack Name
         | Stack Status    |
    +--------------------------------------+--------------------------
    -----+-----------------+
    | 6c3fcfca-46e3-4dd2-a887-e0ea4ff7258b | vio567_network_security_gr
    oup   | CREATE_COMPLETE |
    | 668dbe5f-8041-4fd7-a822-c0592ce000fc | vio567_VNFLCM
         | CREATE_COMPLETE |
    | 02c764fa-6008-4749-a37f-d193ae8c2c68 | vio567_vnflcm_security_gro
    up    | CREATE_COMPLETE |
    +--------------------------------------+--------------------------
    -----+-----------------+

    [root@vms ~]# openstack server list -c ID -c Name -c Status
    +--------------------------------------+--------------------------
    -+--------+
    | ID                                   | Name
     | Status |
    +--------------------------------------+--------------------------
    ```

```
-+--------+
| 9dc0563e-351f-4bc3-bf2d-4497d5615454 | vio567-vnflaf-services-0    →
 | ACTIVE |
| ab073b0f-8535-410e-b8da-ab2179b1fe1a | vio567-vnflaf-db-0          →
 | ACTIVE |
+--------------------------------------+---------------------------  →
-+--------+

[root@vms ~]# openstack volume  list
+--------------------------------------+---------------------------  →
-+---------+------+---------------------------------------------+
| ID                                   | Display Name                →
 | Status  | Size | Attached to                                 |
+--------------------------------------+---------------------------  →
-+---------+------+---------------------------------------------+
/.../
| 1bd643b7-3618-4cac-b146-7286886a9e42 | vio567-rhel7_iso_volume-0   →
 |available|    5 |                                             |
| 098774d5-7c6c-4ead-bea3-d6b09fccb4b3 | vio567-rhel6vol-0           →
 |available|    5 |                                             |
| c7c64d06-6ed7-44c8-aff7-649375c2f11d | vio567_vnflcm_volume        →
 | in-use  |  120 | Attached to vio567-vnflaf-db-0 on /dev/sdb|
/.../
+--------------------------------------+---------------------------  →
-+---------+------+---------------------------------------------+
```

6.2 Start ENM on Cloud

This section describes how to start ENM on Cloud using either the manage_enm script or the ENM Cloud Management Workflows.

The key difference between the two is that the manage_enm script starts both ENM on Cloud and VNF-LCM VMs, while the ENM Cloud Management Workflows only start ENM on Cloud.

The workflow that starts ENM on Cloud is **Manage ENM - Start**.

Prerequisites:

— ENM on Cloud deployed.

— VNF-LCM deployed.

— ERICenmcloudmgmtworkflows_CXP9036442 RPM is installed on VNF-LCM.

— ERICenmdeploymentworkflows_CXP9034151 RPM installed on VNF-LCM.

— VNF-LCM SED is available.

6.2.1 Start ENM on Cloud Using the manage_enm Script

This section describes how to start ENM on Cloud and the VNF-LCM VMs. VNF-LCM VMs are only started if they are in SHUTOFF state.

Note: The VM or external server hosting the ENM cloud management utils RPM is referred to as the ENM cloud management host.

If the manage_enm script is installed on a Linux distribution that is not based on rpm, it will not be available in the system PATH. Therefore, a full path to the executable must be specified when invoking the script, as shown below:

```
$ <extracted_rpm_directory>/bin/manage_enm start -h
```

Note: Parameter <external_ip_for_services_vm> used in the procedure signifies the VNF-LCM external IP address and corresponds to one of the following values:

- On VNF-LCM High Availability (HA) deployments:

  The <external_ipv4_vip_for_services> or <external_ipv6_vip_for_services> parameter in the VNF-LCM SED.

- On non-HA VNF-LCM deployments:

  The <external_ipv4_for_services_vm> or <external_ipv6_for_services_vm> parameter in the VNF-LCM SED.

The script takes approximately 40 to 50 minutes to complete.

Prerequisites

- ERICenmcloudmgmtutils_CXP9036444 RPM installed on the ENM cloud management host, as described in *Install ENM Cloud Management RPM* in *ENM on Cloud Deployment Instructions* (Available from local Ericsson Support).
- ENM cloud management host can access VNF-LCM's external network.

  Note: For instructions on how to manage access to VNF-LCM, refer to *VNF-LCM Admin CLI (VNF-LCM Security Utility subsection)* in the ENM Configuration System Administrator Guide [21].

- OpenStack RC file for the ENM deployment is available on the ENM cloud management host.
- OpenStack command-line client installed on the ENM cloud management host.
- ENM on Cloud deployment has been successfully shut down using the manage_enm script.
- ENM SED is available.

Steps

1. Log onto the ENM cloud management host.
2. Source the OpenStack RC file for the ENM deployment.

```
$ source <path_to_RC_file>/<name_of_RC_file>.rc
```

Example:

```
$ source /home/enm-admin/enm_deployment.rc
```

3. Display the help message for the script's start action.

```
$ manage_enm start -h
```

Example:

```
$ manage_enm start -h
INFO: Logging to /root/manage_enm.log
usage: manage_enm.py start [-h] [--rcfile RCFILE] [--lcm HOST]
[--lcm-name LCM_NAME] [--lcm-db-name LCM_DB_NAME]
optional arguments:
  -h, --help            show this help message and exit
  --rcfile RCFILE       path to the OpenStack RC file
  --lcm HOST            hostname or IP of VNF-LCM workflow service
  --lcm-name LCM_NAME   Custom value for VNF-LCM services server as defined →
in
                        VNF-LCM SED.
  --lcm-db-name LCM_DB_NAME
Custom value for VNF-LCM DB server as defined in VNF-LCM SED.
```

Note: If the properties <Services_vm_HostName> and <DB_vm_HostName> in the VNF-LCM SED are customized, provide the customized values by using --lcm-name and --lcm-db-name arguments.

4. Start VNF-LCM and ENM using the manage_enm script.

   The script starts the VNF-LCM VMs only if they're in the SHUTOFF state; otherwise, it skips the step. Once the VNF-LCM VMs are in the ACTIVE state, the script runs the **Manage ENM - Start** workflow that starts ENM. The external IP address of the VNF-LCM Services VM must be provided when invoking the script.

```
$ manage_enm start --lcm <external_ip_for_services_vm>
```

Example:

```
[enm-admin@manage-enm-server ~]$ manage_enm start --lcm 10.2.2.1
INFO: Logging to /home/enm-admin/manage_enm.log
INFO: Authenticating with OpenStack
INFO: Checking if essential OpenStack services are up
INFO: Checking if VNF-LCM application is available at "10.2.2.1"
INFO: Starting VNF-LCM servers
INFO: VNF-LCM servers started
```

```
INFO: Waiting for VNF-LCM service to be available
INFO: VNF-LCM service available
INFO: Starting ENM
INFO: Starting StartENM__top workflow
INFO: Monitoring workflow instance StartENM_20181130_152212
.....................................................
INFO: Workflow no longer running
INFO: Workflow instance completed successfully
[enm-admin@manage-enm-server ~]$
```

5. Confirm that the ENM applications are available.

   When the manage_enm script finishes, open the ENM launcher in the browser, using the value that corresponds to the <httpd_fqdn> parameter in the ENM SED, then log in. A list of applications is displayed.

6. Verify that all VNF-LCM and ENM stacks are in the CREATE_COMPLETE state:

   ```
   $ openstack stack list -f value -c 'Stack Status' | grep -iv create_complete
   ```

   The previous command returns no output if all stacks are in the correct state.

7. Verify that all ENM VMs have an entry in Consul.

   a. Find the number of VMs in Consul by logging onto the VNF-LAF Services VM, then running the following command:

      ```
      $ consul members | grep -cv Node
      ```

      Example:

      ```
      [cloud-user@vnflaf-services ~]$ consul members | grep -cv Node
      165
      ```

   b. Find the number of VMs in OpenStack.

      ```
      $ openstack server list -f value -c Name | grep -civ vnflaf-db
      ```

      Note: The previous command excludes the vnflaf-db VM as the Consul agent does not run on this VM.

      Example:

      ```
      [enm-user@manage-enm-server ~]$ openstack server list -f value -c N →
      ame | grep -civ vnflaf-db
      165
      ```

      The number of VMs in Consul should match the number of VMs in OpenStack (excluding the vnflaf-db VM).

6.2.2 Start ENM on Cloud using Cloud Management Workflows

This section describes how to start ENM on Cloud.

This is achieved by running the Manage ENM - Start workflow.

Approximate time to complete the start procedure is 30 to 40 minutes.

Prerequisites

— ENM has been successfully shut down using the **Manage ENM - Shutdown** workflow.

— VNF-LCM UI is available.

Note: Do not run this procedure when performing the steps mentioned in the *ENM Software Upgrade Pre-Steps* and the *ENM Software Upgrade* chapters of the ENM on Cloud Upgrade Instructions document as unexpected errors can occur.

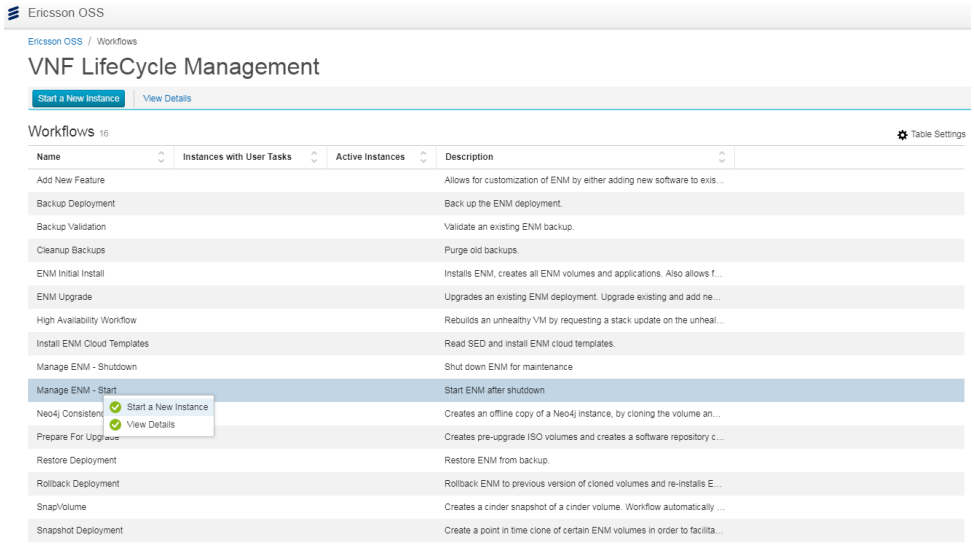
Steps

1. Open the VNF-LCM UI in the browser, using the following URL:

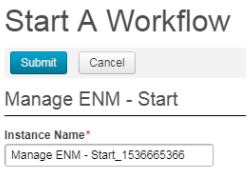
   Note: Replace the value <external_ip_for_services_vm> in the URL with the value corresponding to either the <external_ipv4_vip_for_services> if VNF-LCM deployed in HA Mode or <external_ipv4_for_services_vm> or <external_ipv6_for_services_vm> if VNF-LCM deployed in Non-HA Mode as found on VNF-LCM SED.

   ```
   http://<external_ip_for_services_vm>/index.html#workflows
   ```

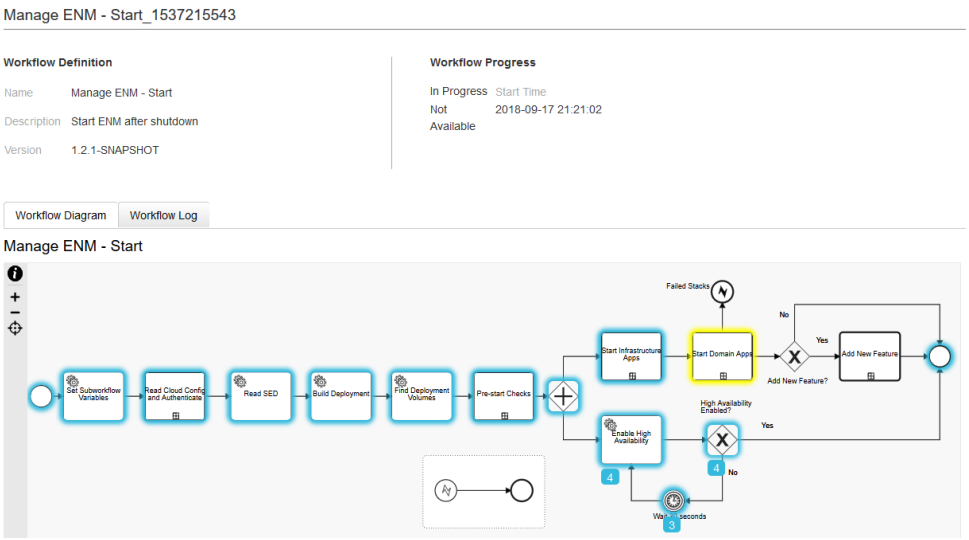
2. Select the **`Manage ENM - Start`** workflow, then click **`Start a New Instance`**. Alternatively, right click the **`Manage ENM - Start`** workflow and select **`Start a New Instance`**.



3. Click **Submit** to start the Manage ENM - Start workflow.

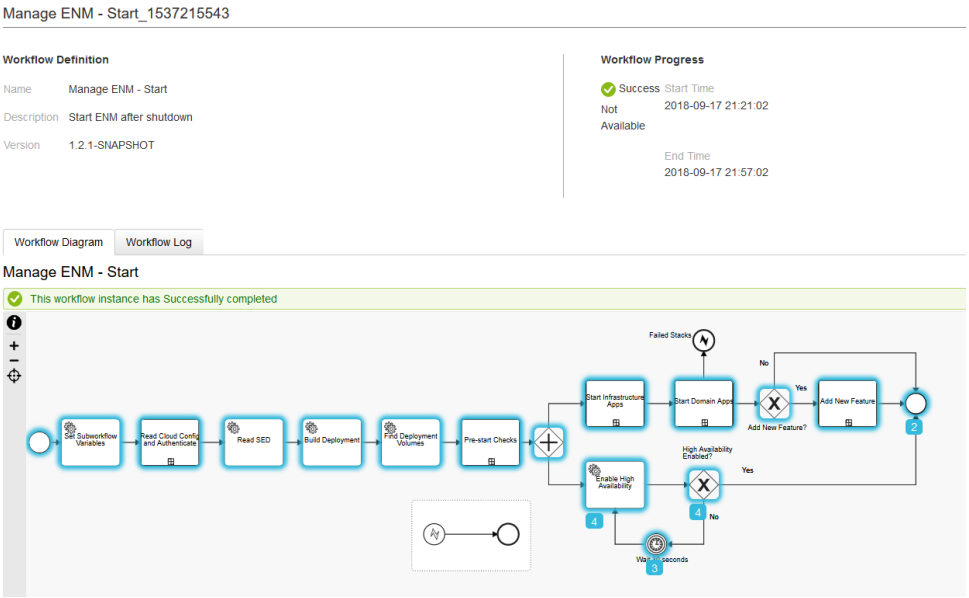


4. Monitor the**Manage ENM - Start** workflow. Use the refresh option to reload and check the progress of the workflow instance.

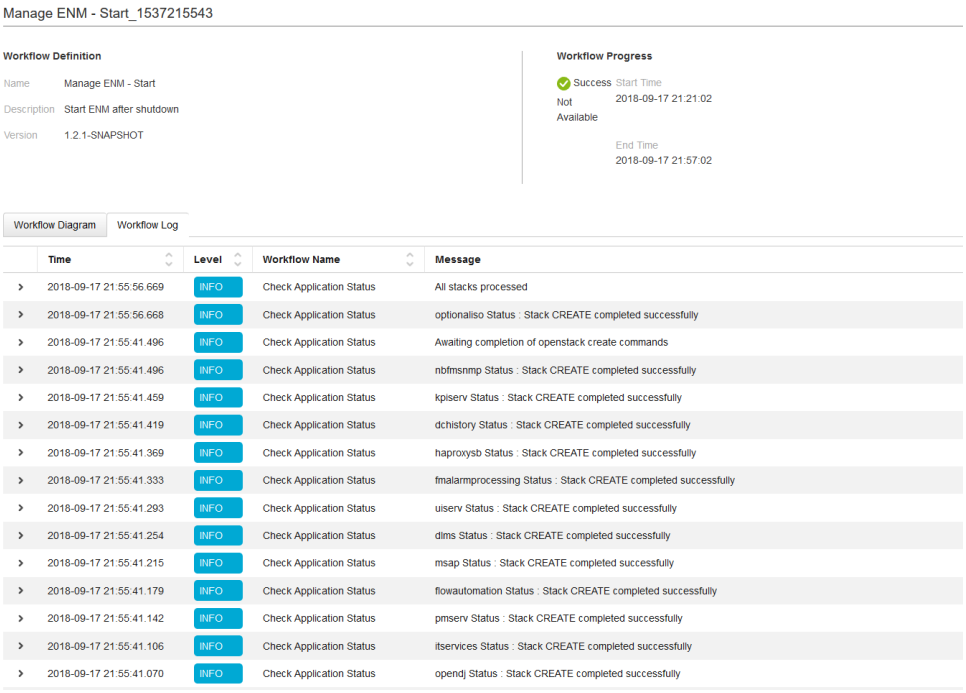


5. Wait for the completion of the**`Manage ENM - Start`** Workflow.

   `Workflow Instance:`



   `Workflow Log:`



6. Gather information about the state of the system after the start:

    a. From an OpenStack client machine source the OpenStack RC file for the ENM on Cloud deployment:

    ```
    # source <OpenStack RC file name>.rc
    ```

    b. Execute the following OpenStack commands to verify the deployment's state:

    ```
    # openstack stack list
    # openstack server list
    # openstack volume list
    ```

    — All stacks should be in the CREATE_COMPLETE state.

    — All servers should be in the ACTIVE state.

    — All volumes should be attached and in the "in-use" state.

    Example:

    ```
    [root@ieatenm3314-str171 ~]# openstack stack list

    +--------------------------------------+------------------------------
    ---+----------------+----------------------+--------------+
    | ID                                   | Stack Name
       | Stack Status    | Creation Time        | Updated Time |
    +--------------------------------------+------------------------------
    ---+----------------+----------------------+--------------+
    | fbe90028-bb7a-                       | ieatenmc7a11_wpserv_f5120752
       | CREATE_COMPLETE | 2018-08-23T14:31:04Z | None         |
    | 4cf2-a042-64953b650536               | -651b-45ee-8a7e-82c5363824f4
    ```

```
   |                      |                              |                  |
| 6f3bce85-913c-                    | ieatenmc7a11_winfiol_aba800c7  →
   | CREATE_COMPLETE | 2018-08-23T14:31:01Z | None         |
| 4e49-9067-5b6162f7a286            | -705a-408d-b403-a465ae140561   →
   |                      |                              |                  |
| f355eaae-4168-4d2a-b33a-          | ieatenmc7a11_visinamingsb_ebd6 →
32 | CREATE_COMPLETE | 2018-08-23T14:30:59Z | None         |
| 56dce9c7f1d6                      | ae-31a9-4870-8c10-492eee3ac160 →
   |                      |                              |                  |
  9cf6795f-3f0b-4aac-               | ieatenmc7a11_visinamingnb_3097 →
85 | CREATE_COMPLETE | 2018-08-23T14:30:57Z | None         |
| aad8-f8d77b68038f                 | c1-8549-499c-9858-64cd74037f0e →
   |                      |                              |                  |
| 94bb7eca-                         | ieatenmc7a11_said_0a6c84f7-7ef →
9  | CREATE_COMPLETE | 2018-08-23T14:30:29Z | None         |
| fb81-462c-a168-ecfb521a06d4       | -4ecf-802a-83d568946a95        →
   |                      |                              |                  |
| bd88746a-d894-4f87-a76c-          | ieatenmc7a11_pmserv_a4298bfa-  →
   | CREATE_COMPLETE | 2018-08-23T14:30:27Z | None         |
| 8a7941dbf8ef                      | 0d80-4fd4-97fb-df5a14315f5b    →
   |                      |                              |                  |
| 1224468f-1a0b-457c-               | ieatenmc7a11_pmrouterpolicy_b3 →
f1 | CREATE_COMPLETE | 2018-08-23T14:30:24Z | None
/.../

[root@ieatenm3314-str171 ~]# openstack server list
+--------------------------+--------------------------+--------
+--------------------------+                                    →
| ID                       | Name                     | Status →
| Networks                 | Image Name               |
+--------------------------+--------------------------+--------
+--------------------------+                                    →
| 78952225-7d4c-4281-81e3-b3 | ieatenmc7a11-winfiol-0     | ACTIVE →
| provider_network2_7A=2001: | ERICrhel6jbossimage_CXP9031 |
| b444f72172                 |                            |        →
| 1b70:6207:85:0:1031:11:2c, | 560-2.53.1_CI.qcow2        |
|                            |                            |        →
| 131.160.142.174; enm_inter |                            |
|                            |                            |        →
| nal_network_Vandals_C7A11= |                            |
|                            |                            |        →
| 10.10.0.222                |                            |
| 7f4e72c9-bcd7-4239-bcd7-14 | ieatenmc7a11-winfiol-1     | ACTIVE →
| provider_network2_7A=2001: | ERICrhel6jbossimage_CXP9031 |
| 72cf76669c                 |                            |        →
| 1b70:6207:85:0:1031:11:2d, | 560-2.53.1_CI.qcow2        |
|                            |                            |        →
| 131.160.142.175; enm_inter |                            |
|                            |                            |        →
| nal_network_Vandals_C7A11= |                            |
|                            |                            |        →
| 10.10.0.223                |                            |
| 1a8821ff-a748-412f-        | ieatenmc7a11-wpserv-1      | ACTIVE →
| enm_internal_network_Vanda | ERICrhel6jbossimage_CXP9031 |
| 90c7-f6c882a9b627          |                            |        →
| ls_C7A11=10.10.0.225       | 560-2.53.1_CI.qcow2        |
| 156c041e-b160-4efc-91fd-   | ieatenmc7a11-wpserv-0      | ACTIVE →
| enm_internal_network_Vanda | ERICrhel6jbossimage_CXP9031 |
| 3b17b6e2e740               |                            |        →
| ls_C7A11=10.10.0.224       | 560-2.53.1_CI.qcow2        |
| 9f77908c-5b04-4b2a-        | ieatenmc7a11-visinamingsb- | ACTIVE →
| provider_network2_7A=2001: | ERICrhel6baseimage_CXP90315 |
| 96b7-7c398de752eb          | 0                          |        →
| 1b70:6207:85:0:1031:11:2a, | 59-2.42.1_CI.qcow2         |
|                            |                            |        →
| 131.160.142.172; enm_inter |                            |
|                            |                            |        →
| nal_network_Vandals_C7A11= |                            |
|                            |                            |        →
| 10.10.0.220                |                            |
 /.../
[root@ieatenm3314-str171 ~]# openstack volume list
+--------------------------------------+------------------------------
-----+--------+------+--------------------------------------+          →
| ID                                   | Display Name                 →
     | Status | Size | Attached to                          |
+--------------------------------------+------------------------------
-----+--------+------+--------------------------------------+          →
| 5157ca90-a974-4dd1-8220-c9aeb7152 | ieatenmc7a11-rhel7_iso_volume →
-0   | in-use |    5 | Attached to ieatenmc7a11-repo-0 on  |
```

```
| 036                                   |                              →
     |        |      | /dev/vdb                                  |
| 0c90c38a-2417-456a-9a0b-              | ieatenmc7a11-rhel7_updates_is →
o_vo  | in-use |    5 | Attached to ieatenmc7a11-repo-0 on  |
| 6820d4c72257                          | lume-0                        →
     |        |      | /dev/vdd                                  |
| 6fa9d15c-b7ec-4c25-8d1b-              | ieatenmc7a11-rhel6vol-0       →
     | in-use |    5 | Attached to ieatenmc7a11-repo-0 on  |
| 0aac883208b1                          |                              →
     |        |      | /dev/vdg                                  |
| 43babe8a-a3d3-45c6-b20b-              | ieatenmc7a11-rhel6_updates_vo →
l-0  | in-use |    5 | Attached to ieatenmc7a11-repo-0 on  |
| f4725ed3290c                          |                              →
     |        |      | /dev/vdf      /.../
```

6.3 Recover ENM on Cloud

This section describes how to use the manage_enm script to recover ENM after loss of service. The script restarts the VNF-LCM VMs if they are not operational. Then it triggers the shutdown and start workflows. The **Manage ENM - Shutdown** workflow is executed with the default (graceful) option which shuts down VMs before deleting stacks. To reduce the load on the deployment, the manage_enm script waits 5 minutes before triggering the **Manage ENM - Start** workflow. The approximate time to recover ENM is 45 to 60 minutes.

Prerequisites

— ENM on Cloud deployed.

— VNF-LCM deployed.

— ERICenmcloudmgmtworkflows_CXP9036442 RPM is installed on VNF-LCM.

— ERICenmdeploymentworkflows_CXP9034151 RPM installed on VNF-LCM.

— ERICenmcloudmgmtutils_CXP9036444 RPM installed on the ENM cloud management host, as described in the *Install ENM Cloud Management RPM* section in the *ENM on Cloud Deployment Instructions* (Available from local Ericsson Support).

— ENM cloud management host is allowed to access VNF-LCM's external network.

Note: For instructions on how to manage access to VNF-LCM, refer to *VNF-LCM Admin CLI (VNF-LCM Security Utility subsection)* in the ENM Configuration System Administrator Guide [21].

— OpenStack RC file for the ENM deployment is available on the ENM cloud management host.

— VNF-LCM and ENM SEDs are available.

Steps

1. Log onto the ENM cloud management host.
2. Source the OpenStack RC file for the ENM deployment.

   Example

   ```
   $ source /root/enm_123_project.rc
   ```

3. Display the help message for the script's recover action.

   ```
   $ manage_enm recover --help
   ```

   Example

   ```
   $ manage_enm recover --help
   INFO: Logging to /root/manage_enm.log
   usage: manage_enm.py recover [-h] [--rcfile RCFILE] [--lcm HOST]
                                [--lcm-name LCM_NAME] [--lcm-db-name LCM_DB_NAM →
   E]
                                [--reason REASON]

   optional arguments:
     -h, --help            show this help message and exit
     --rcfile RCFILE       path to the OpenStack RC file
     --lcm HOST            hostname or IP of VNF-LCM workflow service
     --lcm-name LCM_NAME   Custom value for VNF-LCM services server as defined  →
   in
                           VNF-LCM SED.
     --lcm-db-name LCM_DB_NAME
                           Custom value for VNF-LCM DB server as defined in VNF →
   -
                           LCM SED.
     --reason REASON       reason for recovery of ENM
   ```

   Note: If the properties <Services_vm_HostName> and <DB_vm_HostName> in the VNF-LCM SED are customized, provide the customized values by using --lcm-name and --lcm-db-name arguments.

4. Execute the manage_enm script with the recover option

   ```
   $ manage_enm recover
   ```

   Example

   ```
   $ manage_enm recover --reason "Recover ENM after loss of service"
   INFO: Logging to /root/manage_enm.log
   INFO: Recover ENM started
   INFO: Authenticating with OpenStack
   INFO: Checking if essential OpenStack services are up
   INFO: Checking if VNF-LCM workflows are available at "vnflaf-services"
   INFO: Starting ShutdownENM__top workflow
   INFO: Monitoring workflow instance ShutdownENM_20181011_101425
   ............
   INFO: Workflow no longer running
   INFO: Workflow instance completed successfully
   INFO: Waiting 300 seconds before starting ENM
   INFO: Authenticating with OpenStack
   INFO: Checking if essential OpenStack services are up
   INFO: Checking if VNF-LCM application is available at "vnflaf-services"
   INFO: Starting ENM
   ```

```
INFO: Starting StartENM__top workflow
INFO: Monitoring workflow instance StartENM_20181011_102557
.............................................................
INFO: Workflow no longer running
INFO: Workflow instance completed successfully
```

Note: Providing a reason for recovery is optional. If not provided, the default reason, "manage_enm - Recover ENM after unexpected downtime", is passed to Manage ENM - Shutdown workflow.

5. Gather information about the state of the system after the recovery:

    a. Confirm that the ENM applications are available:

    When the manage_enm script finishes, open the ENM launcher in the browser, using the value that corresponds to the <httpd_fqdn> parameter in the ENM SED, then log in. A list of applications should be displayed in the ENM Application Launcher.

    b. Verify that all VNF-LCM and ENM stacks are in the CREATE_COMPLETE state:

    ```
    $ openstack stack list -f value -c 'Stack Status' | grep -iv create
    _complete
    ```

    Note: The previous command returns no output if all stacks are in the correct state.

    c. Verify that all VNF-LCM and ENM VMs are in the ACTIVE state:

    ```
    $ openstack server list -f value -c Name -c Status | grep -iv activ
    e
    ```

    Note: The previous command returns no output if all VMs are in the correct state

    d. Verify that all ENM volumes are in the in-use state:

    ```
    $ openstack  volume list -f value -c "Display Name" -c Status | gre
    p -iv in-use
    ```

    Note: The previous command returns no output if all volumes are in the correct state.

    e. Verify that all ENM VMs have an entry in Consul:

    Find the number of VMs in Consul by logging onto the VNF-LAF Services VM, then running the following command:

    ```
    $ consul members | grep -cv Node
    ```

Example

```
[cloud-user@vnflaf-services ~]$ consul members | grep -cv Node
165
```

f. Find the number of VMs in OpenStack.

```
$ openstack server list -f value -c Name | grep -civ vnflaf-db
```

Note: The previous command excludes the vnflaf-db VM as the Consul agent does not run on this VM.

Example

```
[enm-user@manage-enm-server ~]$ openstack server list -f value -c N →
ame | grep -civ vnflaf-db
165
```

The number of VMs in Consul should match the number of VMs in OpenStack (excluding the vnflaf-db VM).

Result: ENM is successfully recovered.

6.4 Procedure for Updating VNF-LCM keypair

Describes how to update key-pair on VNF-LCM with current software baseline.

Prerequisites

— Access to `keystonerc` file for the deployment.

— Access to the VNF-LCM Upgrade Instructions (available from local Ericsson Support), refer to Release Note for correct revision to use for a deployment.

— Access to the ENM on Cloud Upgrade Instructions (available from local Ericsson Support), refer to Release Note for correct revision to use for a deployment.

— Existing deployed software images are available on glance.

— Access to a client machine to run openstack operation; on the Small Integrated ENM solution the VMS should be used as the client machine.

Steps

Complete the following, depending on deployment type:

— Procedure for Updating keypair on VNF-LCM deployed on OpenStack or CEE on page 211 where deployment type is Openstack or CEE.

— Procedure for Updating key-pair on VNF-LCM Deployed on VIO on page 213 where deployment type is SIENM.

Expected Result

Keypair is updated successfully on VNF-LCM.

6.4.1 Procedure for Updating keypair on VNF-LCM deployed on OpenStack or CEE

How to update key-pair on VNF-LCM deployed on OpenStack or CEE.

Prerequisites

— This procedure assumes access to VNF-LCM Services VM using a known password and upgrade to same software is being performed to achieve keypair update.

— Access to `keystonerc` file for the deployment.

— Steps in *Create New keypair on an ENM on Cloud Deployment* completed where VNF-LCM is integrated with ENM on Cloud.

— Steps in *Create New keypair for VNF-LCM* completed where VNF-LCM is integrated with OSSRC, ENM or Ericsson Orchestrator(EO).

— VNF-LCM access details available.

— Access to the VNF-LCM Upgrade Instructions (available from local Ericsson Support), refer to Release Note for correct revision to use for an deployment.

— Access to the ENM on Cloud Upgrade Instructions (available from local Ericsson Support), refer to Release Note for correct revision to use for an deployment.

— Existing deployed software images are available in glance.

Expected Result

Keypair is updated successfully on VNF-LCM deployed on OpenStack or CEE.

6.4.1.1 HA Deployment of VNF-LCM

Steps

1. Log on to the client machine and set the environment with your `keystonerc` file.

2. Perform steps in *Create Volume Backups for Rollback in OpenStack or CEE* in VNF-LCM Upgrade Instructions.

3. Perform steps in *Retrieve VNF-LCM From State Artifacts for OpenStack or CEE* in VNF-LCM Upgrade Instructions.

Depending on the OSS type, update the `vnflcm_sed.json` file downloaded in Step 3 with new keypair name as created in:

— *Create New keypair on an ENM on Cloud Deployment* in ENM on Cloud Upgrade Instructions where VNF-LCM is integrated with ENM on Cloud.

— *Create New keypair for VNF-LCM* in VNF-LCM Upgrade Instructions where VNF-LCM is integrated with OSSRC, ENM, or Ericsson Orchestrator (EO).

Then proceed to Step 4

4. Perform steps in *Update HA Security Group in OpenStack or CEE* in VNF-LCM Upgrade Instructions.

5. Perform steps in *Update HA Server Group in OpenStack or CEE* in VNF-LCM Upgrade Instructions.

6. Perform steps in *Upgrade the VNF-LCM in OpenStack, CEE or VIO* in VNF-LCM Upgrade Instructions.

7. Verify `keypair` is updated:

```
# openstack stack show <deployment_id>_VNFLCM | grep -i keypair
# openstack server show <deployment_id>-vnflaf-services-0 | grep -i key_name
# openstack server show <deployment_id>-vnflaf-db-0 | grep -i key_name
```

The <deployment_id> is the value of the deployment_id in the SED.

Example:

```
# openstack stack show C4B06_VNFLCM | grep -i keypair
| | keypair: 4B06_key_new |
# openstack server show C4B06-vnflaf-services-0 | grep -i key_name
| key_name | 4B06_key_new |
# openstack server show C4B06-vnflaf-db-0 | grep -i key_name
| key_name | 4B06_key_new
```

Note: Example commands given are executed on VNF-LCM Non-HA deployment.

On failure refer to *VNF-LCM Rollback in OpenStack, CEE or VIO* in VNF-LCM Upgrade Instructions

6.4.1.2 Non-HA Deployment of VNF-LCM

Steps

1. Log on to the client machine and set the environment with your `keystonerc` file.
2. Perform steps in *Create Volume Backup for Rollback in OpenStack or CEE* in VNF-LCM Upgrade Instructions.
3. Perform steps in *Retrieve VNF-LCM From State Artifacts for OpenStack or CEE* in VNF-LCM Upgrade Instructions.

Depending on the OSS type, update the `vnflcm_sed.json` file downloaded in Step 3 with new keypair name as created in:

— *Create New keypair on an ENM on Cloud Deployment* in ENM on Cloud Upgrade Instructions where VNF-LCM is integrated with ENM on Cloud.

— *Create New keypair for VNF-LCM* in VNF-LCM Upgrade Instructions where VNF-LCM is integrated with OSSRC, ENM, or Ericsson Orchestrator (EO).

Then proceed to Step 4

4. Perform steps in *Update Security Group in OpenStack or CEE* in VNF-LCM Upgrade Instructions.
5. Perform steps in *Update Server Group in OpenStack or CEE* in VNF-LCM Upgrade Instructions.
6. Perform steps in *Upgrade the VNF-LCM in OpenStack, CEE or VIO* in VNF-LCM Upgrade Instructions.
7. Verify `keypair` is updated:

```
# openstack stack show <deployment_id>_VNFLCM | grep -i keypair
# openstack server show <deployment_id>-vnflaf-services-0 | grep -i key_name
# openstack server show <deployment_id>-vnflaf-db-0 | grep -i key_name
```

The <deployment_id> is the value of the deployment_id in the SED.

Example:

```
# openstack stack show C4B06_VNFLCM | grep -i keypair
 | | keypair: 4B06_key_new |
 # openstack server show C4B06-vnflaf-services-0 | grep -i key_name
 | key_name | 4B06_key_new |
 # openstack server show C4B06-vnflaf-db-0 | grep -i key_name
 | key_name | 4B06_key_new
```

6.4.2 Procedure for Updating key-pair on VNF-LCM Deployed on VIO

Prerequisites

— This procedure assumes access to VNF-LCM Services VM using a known password and upgrade to same software is being performed to achieve keypair update.

— Access to `keystonerc` file for the deployment.

— Steps in *Create New keypair on an ENM on Cloud Deployment* in ENM on Cloud Upgrade Instructions completed where VNF-LCM is integrated with ENM on Cloud.

— VNF-LCM access details available.

— Access to the VNF-LCM Upgrade Instructions (available from local Ericsson Support), refer to Release Note for correct revision to use for an deployment.

— Access to the ENM on Cloud Upgrade Instructions (available from local Ericsson Support), refer to Release Note for correct revision to use for an deployment.

— In the Small Integrated ENM solution the VMS should be used as the client machine.

— Existing deployed software images are available in glance.

Steps

1. Log on to the client machine and set the environment with your `keystonerc` file.
2. Perform steps in *Create Volume Backup for Rollback in VIO* in VNF-LCM Upgrade Instructions.
3. Perform steps in *Retrieve VNF-LCM From State Artifacts for VIO* in VNF-LCM Upgrade Instructions.
4. Update the `vnflcm_sed.json` file downloaded in Step 3 with new keypair name as created in *Create New keypair on an ENM on Cloud Deployment* in ENM on Cloud Upgrade Instructions.
5. Perform steps in *Update Security Group in VIO* in VNF-LCM Upgrade Instructions.
6. Perform steps in *Update Server Group in VIO* in VNF-LCM Upgrade Instructions.
7. Perform Steps in *Upgrade the VNF-LCM in OpenStack, CEE or VIO* in VNF-LCM Upgrade Instructions.
8. Verify keypair is updated.

```
# openstack stack show <deployment_id>_VNFLCM | grep -i keypair
# openstack server show <deployment_id>-vnflaf-services-0 | grep -i key_name
# openstack server show <deployment_id>-vnflaf-db-0 | grep -i key_name
```

Example:

```
# openstack stack show C4B06_VNFLCM | grep -i keypair
| | keypair: 4B06_key_new |
# openstack server show C4B06-vnflaf-services-0 | grep -i key_name
| key_name | 4B06_key_new |
# openstack server show C4B06-vnflaf-db-0 | grep -i key_name
| key_name | 4B06_key_new
```

Note: On failure refer to *VNF-LCM Rollback in OpenStack, CEE or VIO* in VNF-LCM Upgrade Instructions.

6.5 Procedure for Upgrading ENM on Cloud keypair.

How to upgrade key-pair on a ENM on Cloud deployment with current software baseline.

Prerequisites

— Access to keystonerc file for the deployment.

— Access to the VNF-LCM Upgrade Instructions 1/153 72-CNA 403 3313, refer to Release Note for correct revision to use for a deployment.

— Access to the ENM on Cloud Upgrade Instructions 2/153 72-AOM 901 151, refer to Release Note for correct revision to use for a deployment.

— Images belonging to current software baseline deployed are available in glance.

— Access to a client machine to run openstack operations, on the Small Integrated ENM solution the VMS should be used as the client machine.

— New Keypair created and available to update deployment. As needed Request creation of new tenancy's private key from your OpenStack administrator. Refer Appendix II - Update Keypair on an ENM on Cloud Deployment from "ENM on Cloud Upgrade Instructions" document.

— VNF-LCM is updated successfully with new keypair. Refer Procedure for updating VNF-LCM keypair

Steps

Complete the following in sequence:

1. Complete steps on Upgrade ENM on Cloud Deployment with new key-pair.

2. Complete steps on Verify ENM on Cloud Deployment is accessible with new keypair post successful upgrade.

3. Complete "Post Upgrade Steps for ENM on Cloud" chapter from "ENM on Cloud Upgrade Instructions" document as applicable to deployment type.

4. Cleanup of old keypair should only be done when keypair is not used by any active running server on a cloud deployment.

Note: If unsure do not delete a keypair and contact your OpenStack administrator for keypair cleanup as needed.

6.5.1 Upgrade ENM on Cloud Deployment with new key-pair.

How to upgrade key-pair on a ENM on cloud deployment with current software baseline

Prerequisites

— Access to keystonerc file for the deployment.

— New keypair is created and available on an ENM on Cloud deployment.

— VNF-LCM is successfully upgraded using New keypair and VNF-LCM access details are available. Refer Procedure for updating VNF-LCM keypair

— In the Small Integrated ENM (VIO) solution the VMS should be used as the client machine.

Steps

1. Follow *Check the OpenDJ Replication Status* in ENM on Cloud Upgrade Instructions to confirm health of OpenDJ replication.

2. Follow *Create Rollback Snapshots for ENM Deployment* in ENM on Cloud Upgrade Instructions to take a snapshot of the system.

3. Follow *Check the OpenDJ Replication Status* in ENM on Cloud Upgrade Instructions to confirm health of OpenDJ replication post snapshot.

4. Refer to *How To* section in Site Engineering Data for ENM on Cloud to import already existing sed.json.

   Once imported manually update the <key_name> field with newly created keypair value as part of prerequisite step and generate new sed.json file.

   Note: When existing sed.json is imported into Site Engineering Data for ENM on Cloud, user should manually update the <key_name> field with newly created key when generating new sed.json for upgrade. User needs to manually verify updated key correctly is used on this field as there is no automated validation for this on SED.

Note: VNF-LCM service VM should already be updated at this point and user should be able to login to VNF-LCM services VM using the new pem file.

Access VNF-LCM services VM using External IP address referred to as <external_ip_for_services_vm> throughout this document.

When access VNF-LCM Non-HA deployments <external_ip_for_services_vm> should be replaced with value defined for <external_ipv4_for_services_vm> or <external_ipv6_for_services_vm> fields on VNF-LCM SED.

When access VNF-LCM HA deployments <external_ip_for_services_vm> should be replaced with value defined for <external_ipv4_vip_for_services> or <external_ipv6_vip_for_services> fields on VNF-LCM SED.

5. Complete the following steps to transfer new sed.json to vnf-lcm.

    a. Log in to the VNF-LCM services VM as <cloud-user> using the new values defined for <key_name> defined in the SED , Refer following examples use correct value for <external_ip_for_services_vm> based on VNF-LCM deployment type.

    ```
    # scp -i <new_keypair>.pem new_enm_sed.json cloud-user@<external_ip →
    _for_services_vm>:/var/tmp/
    ```

    b. Backup existing sed.json file on VNF-LCM /vnflcm-ext/enm/ path and update with new_sed.json transfered in previous step.

    ```
    [cloud-user@vnflaf-services ~]$ sudo -i

    [root@vnflaf-services-0 ~]# cp /vnflcm-ext/enm/sed.json /vnflcm-ext →
    /enm/sed.json.bkup

    [root@vnflaf-services-0 ~]# cp /var/tmp/new_enm_sed.json /vnflcm-ex →
    t/enm/sed.json
    ```

    c. Verify new keypair name has been updated on the sed.json file.

    ```
    [root@vnflaf-services-0 ~]# diff sed.json sed.json_bkup
    ```

    Example:

    ```
    [root@ieatenm7a02-vnflaf-services-0 ~]# diff sed.json sed.json_bkup
    14c14
    < "key_name":"new_enm_keypair",
    ---
    > "key_name":"enm_keypair",
    ```

6. Follow *Run Pre-Upgrade Step for Model Deployment* in ENM on Cloud Upgrade Instructions.

7. Follow *Prepare for Upgrade Workflow* in ENM on Cloud Upgrade Instructions.

8. Follow *Pre-Upgrade Step for Data Persistence Service (DPS)* in ENM on Cloud Upgrade Instructions.
9. Follow *Pre-Upgrade Steps for GEO-R* in ENM on Cloud Upgrade Instructions if applicable else skip.
10. Follow *Upgrade ENM on Cloud Using VNF-LCM* in ENM on Cloud Upgrade Instructions.

6.5.2 Verify ENM on Cloud Deployment is Accessible with New keypair Post Upgrade

How to upgrade key-pair on a ENM on cloud deployment with existing software.

Prerequisites

- Access to keystonerc file for the deployment.
- VNF-LCM is successfully upgraded using new keypair. and VNF-LCM access details available.
- Steps in Upgrade ENM on Cloud Deployment with new key-pair. on page 216 completed successfully.
- In the Small Integrated ENM solution the VMS should be used as the client machine.

Steps

1. Log in to the EMP VM as cloud-user using the pem file for new keypair.

```
# ssh -i <new_key_name>.pem cloud-user@<emp_external_ip_list>
```

Example:

```
# ssh -i new_enm_keypair.pem cloud-user@131.160.141.74
Warning: Permanently added '131.160.141.74' (RSA) to the list of known hosts →
.
Last login: Thu Mar 28 14:30:18 2019 from 159.107.167.164
[cloud-user@ieatenm7a02-emp-0 ~]$ exit
logout
Connection to 131.160.141.74 closed.
```

2. If login is successful, the new keypair is upgraded on the deployment and this procedure to upgrade keypair is complete, proceed to perform all applicable *Post Upgrade Steps for ENM on Cloud* as defined in ENM on Cloud Upgrade Instructions.

Note: If unable to login using the new keypair, verify the correct pem file is being used and that the correct permissions are set on the file. If the upgrade procedure or verification of the new keypair post upgrade has failed it will require rollback to restore ENM with old keypair.

Refer to *Rollback ENM on Cloud* in ENM on Cloud Upgrade Instructions to perform ENM rollback. Refer to the appropriate VNF-LCM rollback sections as needed for vnf-lcm rollback.

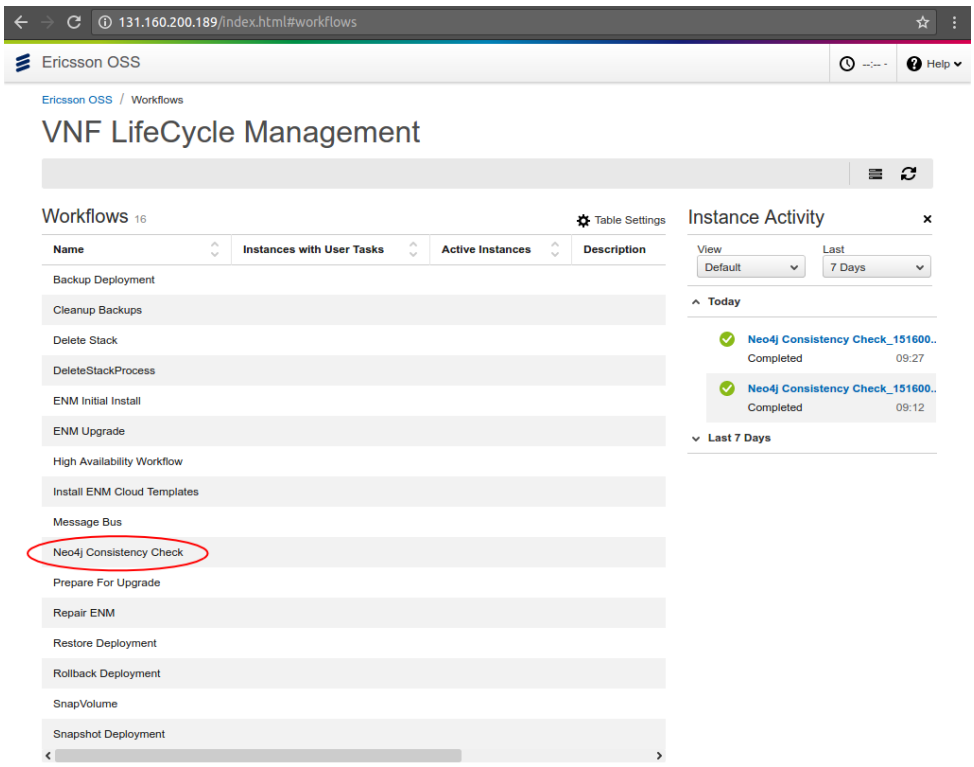
6.6 Neo4j Consistency Check Workflow

Inconsistencies in the Neo4j database are extremely rare. Neo4J provide a Consistency Checker which is implemented via the "Neo4j Consistency Check Workflow". Consistency Checking is essentially part of Neo4J Backup Validation. On very rare occasions, it may be necessary to run a Neo4J Consistency Check on demand on the Neo4J Deployment.

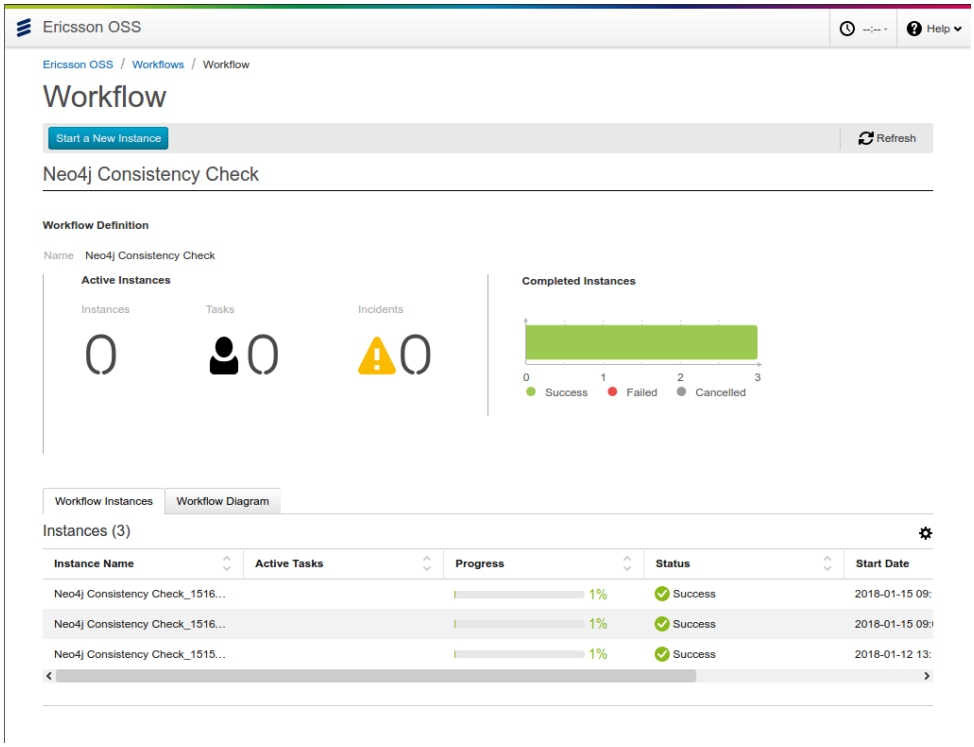
To avoid false positives and to ensure current performance is not impacted, the ENM implementation of Neo4J Consistency Check spawns a new temporary Instance of Neo4J. The Database used for the Consistency Checker is a snapshot copy of the current active Neo4J Database, and the Neo4J Consistency Check is performed on this database copy with Neo4J offline on the new temporary instance.

Steps

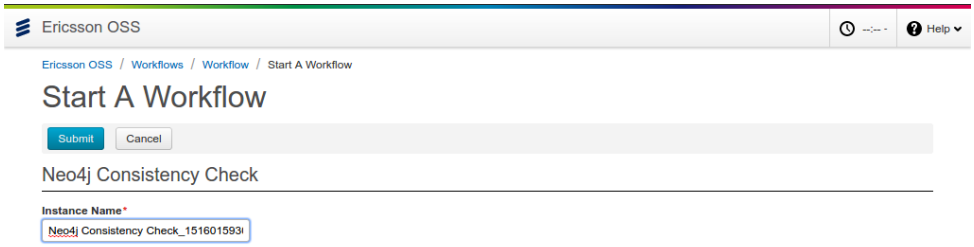
1. A section called **Neo4j Consistency Check** is part of the workflow list under VNF Lifecycle Management, as illustrated by the image below. To execute it, double-click **Neo4j Consistency Check**:



2. A new page is displayed. Click on the blue button **Start a New Instance** as shown in the following image:



3. This displays a form with a single field for the name of this instance execution. A predefined name with the current time stamp is generated, but the user can change it. Click the **submit** button to start the workflow:



   a. Pick one of the Neo4j instances to use as the base to perform the Consistency Check.

   b. Check if a snapshot already exists for the above instance, if not, create it and wait until it is successfully created.

   c. Create a volume based on the snapshot and wait until it is successfully created.

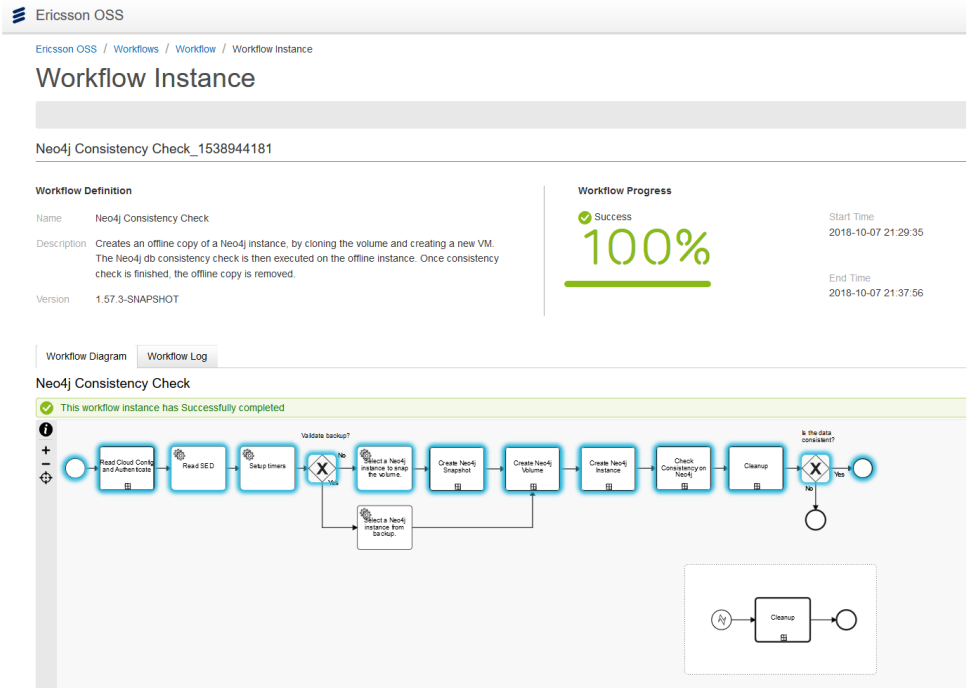
   d. Create a new Neo4j instance with the above volume attached to it. Wait for its creation to complete.

   e. Runs the "Consistency Check" "neo4j-admin" tool on the new Neo4j instance.

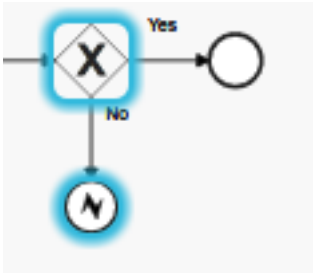
   f. Perform a Cleanup. Delete the new Neo4j Instance along with its volume and snapshot.

   g. Returns the actual Consistency Check result executed in step 5: success or failure.

4. The image below illustrates a successful execution of the **Neo4j Consistency Check Workflow**:



If inconsistencies in the database are found, the final step of the diagram workflow reports failure as opposed to a successful execution:



Note: If Consistency Check Failure persists, contact Local Ericsson Support.

Neo4J Consistency Check can also be used for backup validation as described in *Validate a Backup* in the *ENM on Cloud Backup and Restore Administrators Guide*.

If Consistency Check Failure persists, contact Local Ericsson Support. If the consistency check failure is due to inconsistencies in the Neo4j data, a report file with detailed information is generated at `/ericsson/tor/data/neo4j/cc_reports/`, accessible via any Neo4j VM.

6.7 Elasticsearch Database Administration on ENM on Cloud Deployments

The `Elasticsearch Administration` script is available on the `elasticsearch vm` under `/opt/ericsson/elasticsearch/elasticsearch_admin.py`.

It is used as a troubleshooting or general information utility.

Prerequisites

— Access to the elasticsearch vm on cloud.

Note: Private key is needed to access elasticsearch vm.

— Access as the `es_admin` user.

- Log on to the elasticsearch service and switch user to `es_admin`.

```
[root@meghaenm010218-elasticsearch-0 ~]# su es_admin
```

Note: Post upgrade, the user and group permissions of the export path which are configured during the `Log export configuration` and `Export audit logs options` must be `es_admin:es_admin`.

If in any case permissions for user and group for log export path is not `es_admin:es_admin`. Manual work around is required.

To check the user and group permissions, execute the following command:

```
[root@meghaenm010218-elasticsearch-0 ~]$ ls -ld /ericsson/enm/dumps/exp →
ort_logs_every_5_minutes_with_retention_1_hours
drwxr-xr-x. 2 es_admin es_admin 8192 Jun 16 14:00 /ericsson/enm/dumps/e →
xport_logs_every_5_minutes_with_retention_1_hours
```

To change the user and group permissions to `es_admin:es_admin`, execute the following steps:

1. Log on to the elasticsearch service and switch user to `root`.
2. Change permissions to `es_admin:es_admin`:

```
chown -R es_admin:es_admin <absolute export path>
```

For Example:

```
[root@meghaenm010218-elasticsearch-0 dumps]$ chown -R es_admin:es_a →
dmin /ericsson/enm/dumps/export_logs_every_5_minutes_with_retention →
_1_hours
```

6.7.1 Elasticsearch Administration

The script is executable on the elasticsearch VM.

It offers an interactive menu for querying `Elasticsearch` for general information and troubleshooting purposes.

```
[es_admin@meghaenm010218-elasticsearch-0 ~]# python /opt/ericsson/elasticsearch/ →
elasticsearch_admin →
.py

*********************************************************************


ENM - ELASTICSEARCH DBA UTILITY


*********************************************************************


Select the action you want to perform:


0. Quit
1. Version
2. File System
3. Health Check
4. Display Index List
5. Export an Index
6. Run 'remove_err_warn_logs'
7. Manage 'remove_err_warn_logs_cron' Cron Job
8. Terminate 'remove_err_warn_logs_cron.py'
9. Log export configuration(ELECT)
10. Export Audit Logs
11. On demand export of ENM logs


Enter your choice [1-11 or 0 to exit]:
```

The `/opt/ericsson/elasticsearch/elasticsearch_admin.py` script can be executed without the menu, by using the optional parameters set out in Elasticsearch Database Administration Options on page 180.

Selecting option 9 displays the following options:

```
*********************************************************************

LOG EXPORT CONFIGURATION(ELECT)

*********************************************************************


Select the option to perform:

0. Previous menu
1. Create new export policy
2. List existing export policies
3. Manage existing export policies

Enter the option to perform:
```

— Selecting option 1, displays the following:

```
*********************************************************************

CREATE NEW EXPORT POLICY
```

```
**************************************************************************

Enter the export path to be stored (leave empty to consider default path /er →
icsson/enm/dumps):

Select retention period from below options

1. Set retention period for 1 hour
2. Set retention period for 3 hours
3. Set retention period for 6 hours
4. Set retention period for 12 hours

Select retention period for export files (press enter for default log retent →
ion of 12 hours) :
```

Select Frequency Period:

```
Set Log Export Frequency

1. Export previous day index
2. Export logs every 6 hours
3. Export logs every hour
4. Export logs every 15 minutes
5. Export logs every 5 minutes

Select the frequency to export log:
```

- Select any of the options to display the following list of filters:

```
Select a parameter to apply filter to export or press enter to continue  →
with creating policy


You can apply a maximum of two filters to export logs

1. Severity
2. tag
3. hostname
4. program
5. Facility_code
6. Custom_application_logs

Select the filter to apply on export logs:
```

- Selecting option 4, `Program`, displays the following:

  Note: If you enter an incorrect value for the filters program, tag, and hostname then you can use the wildcard option.For example, in the following example the actual value is **JBOSS** but if you entered **JBOSSS**, the script proceeds to use the wildcard. Using this, on entering **JBOS***, all the values that start with JBOS are displayed.

```
Enter value:JBOSSS
Either the value given doesn't have logs or invalid, try using wildcard: →
 JBOS*
     1: JBOSS
enter number:1
```

- Entering the value as **JBOSS** returns a message asking to try using the wildcard **JBOS***. On selecting, option 1: JBOSS from the above displays the following:

```
Select a parameter to apply filter to export or press enter to continue with creating policy

You can apply a maximum of two filters to export logs

1. Severity

2. Tag

3. Hostname

4. Facility_code

5. Custom_application_logs

Select the filter to apply on export logs:
```

- Selecting option 1, `Severity`, displays the following:

```
Select severity to filter

1. Error
2. Info
3. Warning
4. Notice
5. Critical
6. Emergency
7. Alert
8. Debug
0. Previous Menu

Select severity: 5
```

- Selecting option 5, `Critical`, displays the following:

```
Policy created successfully at /opt/ericsson/elasticsearch/policies/export_logs_every_15_minutes_with_retention_1_hours_JBOSS_crit.json

Cron created successfully

Press <RETURN> to continue.
```

Example:

Policy created from previous filter selection:

```
{
"is_enabled": true,
"cron_name": "export_logs_every_6_hours_with_retention_1_hours_JBOSS_crit",
"frequency": [
"0 */06 * * *",
"every 6 hours",
6,
"hours"
],
"wild_card": "program",
"query": {
"program.keyword": "JBOSS",
"severity.keyword": "crit"
},
"export_path": "/ericsson/enm/dumps",
"retention": [
1,
"hours"
]
}
```

Use the `Facility_code`filter to export logs of a specific `facility_code`. Select this filter to get a list of `facility_codes` available for logs in Elasticsearch along with their corresponding facility.

Use the `Custom_application_logs` to export the custom application logs that are sent to Elasticsearch through the `rsyslog conf` files. After you select a `conf` file in by selecting this filter, all the logs that are sent through that `conf` file are exported.

Note:

— After applying the first filter if you want to apply a second filter, the script displays the filter options that are available after the first filter is applied.

If the you select Tag filter with `CROND[<pid>]`, then all the logs with Tag `CROND[pid]` are exported and the policy details are updated as `"wild_card": "CROND$"`. If you do not have the required value of the filter even after display of wildcard, press **i** and give the filter name and the script creates the policy.

If you use a `wild_card`, the script updates the `wild_card` in the policy file with the filter applied, else the policy file is not updated. For example, in the policy file :`"wild_card": "program"`.

If the first filter `Program = neo4j_debug_log` is applied to a policy and you want to apply the Hostname as the second filter for policy creation, then the script displays the possible Hostnames that are available after applying the `Program` filter, as shown in the following example:

```
Select the frequency to export log: 3

Select a parameter to apply filter to export or press ente →
r to continue with creating policy

You can apply a maximum of two filters to export logs

1. Severity
2. tag
3. hostname
4. program
5. Facility_code
6. Custom_application_logs

Select the filter to apply on export logs: 4
Enter value:Neo4j
Either the value given doesn't have logs or invalid, try u →
sing wildcard(Eg-CRON*): neo4*
1: neo4j_txn_log_retention_update 3: neo4j_dps_script_exec →
 5: neo4j_availability_check
2: neo4j_debug_log 4: neo4j_log 6: neo4j_data_monitor
enter number or press i to provide a user defined value:3

Select a parameter to apply filter to export or press ente →
r to continue with creating policy

You can apply a maximum of two filters to export logs

1. Severity
2. tag
3. hostname
4. Facility_code
5. Custom_application_logs

Select the filter to apply on export logs:
Select the filter to apply on export logs: 3
1: cloud-db-1
enter number or press i to provide a user defined value:1

Policy created successfully at /opt/ericsson/elasticsearch →
/policies/export_logs_every_hour_with_retention_1_hours_ne →
o4j_dps_script_exec_cloud-db-1.json

Cron created successfully

Press <RETURN> to continue..
```

— Logs exported to export file will be in csv format.

Order of **Headers** for each field in each message in the export file are as follows:

1. severity code

— Selecting option 2 in this sub-menu lists the policies present to export logs:

Note: You can create only two export policies excluding the audit policy. Maximum three policies can be created,one audit policy and two generic policies.

```
**************************************************************************

LIST EXISTING EXPORT POLICIES

**************************************************************************



Select the policy option
1. export_logs_every_6_hours_with_retention_1_hours_JBOSS_crit.json
2. export_logs_every_hour_with_retention_1_hours_neo4j_dps_script_exec_cloud →
-db-1.json

Select the option to view current policy details: 1
{
"is_enabled": true,
"disabled_time": "2020-07-28 10:37:47.037259",
"retention": [
1,
"hours"
],
"frequency": [
"0 */06 * * *",
"every 6 hours",
6,
"hours"
],
"wild_card": "program",
"query": {
"program.keyword": "JBOSS",
"severity.keyword": "crit"
},
"export_path": "/ericsson/enm/dumps",
"cron_name": "export_logs_every_6_hours_with_retention_1_hours_JBOSS_crit"
}


Press <RETURN> to continue..
```

Note: The export of logs from the time you disabled can be applied only to export the logs of the current day. It does not include the logs of the previous or any other days before.

— Selecting option 3 displays the following:

```
Select the option to perform:

0. Previous menu
1. Disable existing export policies
2. Enable existing export policies
3. Remove existing export policies

Enter the option to perform:
```

- Selecting option 1 disables the policy to stop exporting logs:

```
Select the policy option
1. export_logs_every_6_hours_with_retention_1_hours_JBOSS →
_crit.json
2. export_logs_every_hour_with_retention_1_hours_neo4j_dp →
```

```
s_script_exec_cloud-db-1.json

Select the option to view current policy details: 1
{
"is_enabled": true,
"disabled_time": "2020-07-28 10:37:47.037259",
"retention": [
1,
"hours"
],
"frequency": [
"0 */06 * * *",
"every 6 hours",
6,
"hours"
],
"wild_card": "program",
"query": {
"program.keyword": "JBOSS",
"severity.keyword": "crit"
},
"export_path": "/ericsson/enm/dumps",
"cron_name": "export_logs_every_6_hours_with_retention_1_ →
hours_JBOSS_crit"
}

Are you sure you want to disable the policy? [Y/n] :y


Selected policy export_logs_every_5_minutes_with_retentio →
n_12_hours_JBOSS_crit.json disabled successfully


Press <RETURN> to continue..
```

- Selecting option 2 enables the policy to export logs:

```
Select the policy option
1. export_logs_every_5_minutes_with_retention_12_hours_JBOSS_crit.json
2. export_logs_from_previous_day_index_with_retention_12_hours_security. →
json

Select the option to view current policy details:2

{
"is_enabled": false,
"disabled_time": "2020-07-28 10:37:47.037259",
"retention": [
1,
"hours"
],
"frequency": [
"0 */06 * * *",
"every 6 hours",
6,
"hours"
],
"wild_card": "program",
"query": {
```

```
"program.keyword": "JBOSS",
"severity.keyword": "crit"
},
"export_path": "/ericsson/enm/dumps",
"cron_name": "export_logs_every_6_hours_with_retention_1_hours_JBOSS_cri →
t"
}

Are you sure you want to re-enable the policy? [Y/n] :y

Do you want export logs from the time you disabled? [Y/n]: y


Selected policy export_logs_every_6_hours_with_retention_1_hours_JBOSS_c →
rit.json enabled successfully


Press <RETURN> to continue..
```

- Selecting option 3 removes the policy to export logs:

```
Enter the option to perform: 3

Select the policy option
1. export_logs_every_6_hours_with_retention_1_hours_JBOSS_crit.json
2. export_logs_every_hour_with_retention_1_hours_neo4j_dps_script_exec_c →
loud-db-1.json

Select the option to view current policy details: 1
{
"is_enabled": true,
"retention": [
1,
"hours"
],
"frequency": [
"0 */06 * * *",
"every 6 hours",
6,
"hours"
],
"wild_card": "program",
"query": {
"program.keyword": "JBOSS",
"severity.keyword": "crit"
},
"cron_name": "export_logs_every_6_hours_with_retention_1_hours_JBOSS_cri →
t",
"export_path": "/ericsson/enm/dumps"
}

Are you sure you want to remove the selected policy ? [Y/n] :y

Cron file removed successfully!

Export policy file removed successfully!


Press <RETURN> to continue..
```

To export Audit logs specifically, select option-10.

Audit logs include the `audit`, `authpriv`, and `syslog` Facility in elasticsearch. You can choose the facility manually. The default facility codes that are exported are; 5, 10, or 13.

You can create only one audit policy at a time. To create a new audit policy, you must delete the existing policy.

You can find the procedure to create an audit log policy from the elasticsearch log admin tool.

Example:

1. In the elasticsearch log admin tool, select option-10:

```
*********************************************************************************

EXPORT AUDIT LOGS

*********************************************************************************
Select option to perform :

1.Set profile for audit logs
2.Export all security log history stored in Elasticsearch index
3.Export security log history with user defined timestamps
4.Export security logs for today(Captures all audit logs in current day ES i →
ndex till current time)
```

2. Select the option to perform. Select option 1 and perform the following steps:

   a. Enter the path where you want the log to be exported. The default path is `/ericsson/enm/dumps`.

   b. Select the retention period for the log export files. The default log retention period is 12 hours:

```
*********************************************************************** →
****

SET SCHEDULED EXPORT POLICY FOR AUDIT LOG

*********************************************************************** →
****



Enter the export path to be stored (leave empty to consider default pat →
h /ericsson/enm/dumps):

Select retention period from below options

1. Set retention period for 1 hour
2. Set retention period for 3 hours
3. Set retention period for 6 hours
4. Set retention period for 12 hours

Select retention period for export files (press enter for default log r →
etention of 12 hours) :
```

   c. Select the frequency to export logs:

```
Set Log Export Frequency

1. Export previous day index
2. Export logs every 6 hours
3. Export logs every hour
4. Export logs every 15 minutes
5. Export logs every 5 minutes

Select the frequency to export log: 5
```

   d. Policy is created successfully. Press **Return** to continue.

```
Policy created successfully at /opt/ericsson/elasticsearch/policies/exp →
ort_logs_every_5_minutes_with_retention_6_hours_security.json

Cron created successfully


Press <RETURN> to continue.
```

3. Select option 2 to export all security logs from the previous elasticsearch indexes:

```
*************************************************************************

EXPORT HISTORICAL AUDIT LOGS RESIDING ON THE DEPLOYMENT

*************************************************************************



Select elasticsearch index from below options :

1. enm_logs-application-2020.07.27
2. enm_logs-application-2020.07.23
3. enm_logs-application-2020.07.24
4. enm_logs-application-2020.07.26

Select index for filtering audit logs : 2

Selected elasticsearch index : enm_logs-application-2020.07.23

Enter export_path (Press enter to consider default path as /ericsson/enm/dum →
ps):

By default facility code 5, 10, 13 logs will be fetched. Do you want to proc →
eed press enter else provide facility codes seperated by (,):

Provide Username to filter audit logs by (press return for none):


Processing request...

Exporting audit logs from enm_logs-application-2020.07.23 index to /ericsson →
/enm/dumps/export_all_security_logs_in_selected_index/2020-07-28-09-59-25.cs →
v.gz

Fetch completed for audit policy...!


Press <RETURN> to continue..
```

4. Select option 3 to export security logs with specific timestamps:

```
************************************************************ →
**************

EXPORT AUDIT LOG HISTORY OF EACH DAY IN SEPARATE FILES

************************************************************ →
**************




Select elasticsearch index from below options :

1. enm_logs-application-2020.07.28
2. enm_logs-application-2020.07.27
```

```
3. enm_logs-application-2020.07.23
4. enm_logs-application-2020.07.24
5. enm_logs-application-2020.07.26

Select index for filtering audit logs : 2

Selected elasticsearch index : enm_logs-application-2020.07.2 →
7

Enter start time of capture (Example format : 05:15:01) : 05: →
01:12

Enter end time of capture (Example format : 10:15:01) : 15:01 →
:05

Enter export_path (Press enter to consider default path as /e →
ricsson/enm/dumps):

By default facility code 5, 10, 13 logs will be fetched. Do y →
ou want to proceed press enter else provide facility codes se →
perated by (,):

Provide Username to filter audit logs by (press return for no →
ne):



Processing request...

Exporting audit logs from enm_logs-application-2020.07.27 ind →
ex to /ericsson/enm/dumps/export_security_logs_for_defined_ti →
mestamps/2020-07-28-09-59-25.csv.gz

Fetch completed for audit policy...!


Press <RETURN> to continue..
```

5. Select option 4 to export security logs from the current ES till the current time:

```
*********************************************************************

EXPORT AUDIT LOGS FOR TODAY

*********************************************************************


Enter export_path (Press enter to consider default path as /ericsson/enm/dum →
ps):

By default facility code 5, 10, 13 logs will be fetched. Do you want to proc →
eed press enter else provide facility codes seperated by (,):

Provide Username to filter audit logs by (press return for none):
```

```
Processing request...

Exporting audit logs from enm_logs-application-2020.07.28 index to /ericsson →
/enm/dumps/export_current_day_security_logs/2020-07-28-11-04-58.csv.gz

Fetch completed for audit policy...!


Press <RETURN> to continue..
```

6. Select option 11 from Elasticsearch DBA tool menu to capture and export ENM logs at one off. Use this feature to:

   - Export ENM logs on demand.
   - Export historical data of the logs in the elasticsearch index from last 1 minute, last 5 minutes, last 15 minutes, last 1 hour, last 3 hours, current day, and previous day.
   - Capture and export filtered ENM logs using the filtering options provided.

   After you select all the options, the log file is generated at the selected export path.

   Example:

```
*********************************************************************

ON DEMAND EXPORT OF ENM LOGS

*********************************************************************



Enter the path for exported logs to be stored (leave empty to consider defau →
lt path /ericsson/enm/dumps):

Select export timeline from below options

1. Export historical data from older ES indices
2. Export current day's data
3. Export last 3 hours data
4. Export last 1 hour data
5. Export last 15 minutes data
6. Export last 5 minutes data
7. Export last 1 minute data

Select export timeline: 5

Select a parameter to apply filter to export or press enter to continue with →
 creating policy

You can apply a maximum of two filters to export logs

1. Severity
2. Tag
3. Hostname
4. Program
5. Facility_code
6. Custom_application_logs

Select the filter to apply on export logs: 1

Select severity to filter

1. Error
2. Info
3. Warning
4. Notice
```

```
5. Critical
6. Emergency
7. Alert
8. Debug
0. Previous Menu

Select severity : 2

Select a parameter to apply filter to export or press enter to continue with
 creating policy

You can apply a maximum of two filters to export logs

1. Tag
2. Hostname
3. Program
4. Facility_code
5. Custom_application_logs

Select the filter to apply on export logs:

Processing Request...

Fetching data...

Fetch completed.

Log File path : /ericsson/enm/dumps/enm-csv-logfile-having_last-15minutes-da
ta_2020-07-15_07-32.gz


Press <RETURN> to continue..
```

6.7.2 Export of Logs with es_admin as a User

> To pull out the exported logs from the export path in elasticsearch service using scp/sftp into an external server, first copy the export files into the vnf laf server and then to the external server.

```
[root@ieatenmc4a06-vnflaf-services-0 tmp]# scp -i /var/tmp/private_key.pemes_adm
in@192.110.8.70:/ericsson/enm/dumps/export_logs_every_5_minutes_with_retention_1
_hours_info/enm-csv-logfile-2020-04-19-07-10-01.gz .
es_admin@192.110.8.70's password:
enm-csv-logfile-2020-04-19-07-10-01.gz 100% 13KB 13.3KB/s 00:00
[root@ieatenmc4a06-vnflaf-services-0 tmp]# ls
enm-csv-logfile-2020-04-19-07-10-01.gz
private_key.pem
systemd-private-747148786d6d4568a81efb1680b16c13-jbcs-httpd24-httpd.service-RqB2
qZ
systemd-private-747148786d6d4568a81efb1680b16c13-ntpd.service-Hfgxpr
```

6.7.3 Elasticsearch Database Administration Options

Option	Description
1) Version	Displays the version of Elasticsearch installed.
2) File System	Displays a summary of Elasticsearch file system information.
3) Health Check	Health status on the health of the cluster.
4) Display Index List	Displays a list of all Elasticsearch indexes along with their size and status.
5) Export an Index	Export the logs of an Elasticsearch index to a `.gz` file in a specified location. Option 4 displays the Elasticsearch indexes size.

Option	Description
	Ensure that the specified location has enough space.
6) Run 'remove_err_warn_logs'	Removes all `err` and `warning` logs of facility local5 greater than seven days old.
7) Manage 'remove_err_warn_logs_cron' Cron Job	Enable or disable the crontab entry `/etc/cron.d/remove_err_warn_logs_cron`.
8) Terminate 'remove_err_warn_logs_cron.py'	If an instance of the `remove_err_warn_logs.py` script is running, this instance of the script is ended. If enabled, the `remove_err_warn_logs.py` is activated in the next crontab. This is, by default, at 1 am the next day. **Note:** This option must be executed before performing an Upgrade.
9) Log export configuration(ELECT)	By running this option, any of the options displayed can be selected that are performed on the data export: 1. `Create export policy`. By selecting this option, the policy file is created as per user selected frequency. Using this policy file, cron performs time-based export of elasticsearch logs in external export path that is mounted to db node. — `Buffer time of 1 minute is maintained to make sure no data is lost.` Example for 5 minutes policy (executed every 0, 5, 10, 15, and so on). If policy is created at 10:18 PM, cron executes at 10:20 PM. In export file, logs are collected starting from 10:14 PM, and last log collected is at 10:19 PM (5 minutes time delta). Buffer time of 1 minute is maintained to allow for writing of logs to elasticsearch. Logs at 10:20 PM are not captured. — `Limitation: Data duplication can occur for 1 minute.` Data may be duplicated for 1 minute, depending on accuracy of cron execution. Example for 5 minutes policy, if cron first executes at 10:20:01 PM, and executes again at 10:25:01 PM, the logs are duplicated at 10:19 PM (logs captured from 10:19 PM to 10:24 PM). 2. `List existing export policies`. By selecting this option, the list of all the created policies is displayed. 3. `Manage export policies`. By selecting this option, the user can Enable, Disable, or Remove a existing cron.
10) Export Audit logs	Execute this option to display the following options that you can select to perform data export. 1. Set profile for security logs This option creates the policy file per the selected frequency. Using this policy file, cron performs a time based export of elasticsearch security logs to an external export path that is mounted on the db node. 2. Export all security log history stored in Elasticsearch index This option exports security logs for the selected elasticsearch index as per user selected facility codes (5, 10, 13). 3. Export security log history with user defined timestamps This option exports the security logs for the selected elastic search index as per user defined time stamps and facility codes. 4. Export security logs for today(Captures all audit logs in current day ES index till current time) This option exports all the security logs for the present day elastic search index as per the user selected facility code.
11) On demand export of ENM logs	Use this option to: — Capture and export ENM logs at one off as per the selected frequency. — Capture and export ENM logs in elasticsearch indices history.

Option	Description
	You can also use the filtering options that are provided to capture and export the filtered logs.

The `/opt/ericsson/elasticsearch/elasticsearch_admin.py` script can be executed without the menu by using the following optional parameters:

```
[es_admin@ieatlms4906 elasticsearch]$ ./elasticsearch_admin.py -h
usage: elasticsearch_admin.py menu [-h] [-v] [-f] [-hc] [-l] [-e] [-r] [-c]
[-dis] [-el] [-a] [-o]

optional arguments:
-h, --help show this help message and exit
-v, --version Elasticsearch Version
-f, --filesystem Elasticsearch File System Info
-hc, --healthcheck Elasticsearch Health Check
-l, --list Display Elasticsearch indices
-e, --export Export Elasticsearch logs
-r, --remove Elasticsearch Delete Error and Warning logs
-c, --cron Elasticsearch Manage Cron Job
-dis, --disable Terminate 'remove_err_warn_logs.py'
-el, --elect Elasticsearch Log Export Configurable Tool
-a, --audit audit_logs
-o, --on_demand One off data export with filtering options
```

```
-elect-audit-policy [-h] --path PATH --log-retention {12 hours,6 hours,3 hours,1 →
 hour}--frequency{previous day index,every 6 hours,every 1 hour,every 5 minutes, →
every minute} , Creates audit policy

Example:

# python elasticsearch_admin.py elect-audit-policy --path "/ericsson/enm/dumps" →
--log-retention "12 hours" --frequency "every 6 hours"

Policy created successfully at /opt/ericsson/elasticsearch/policies/export_logs_ →
every_6_hours_with_retention_12_hours_audit.json
```

```
-elect-create-policy [-h] --path PATH --log-retention {12 hours,6 hours,3 hours, →
1 hour} --frequency {previous day index,every 6 hours,every 1 hour,every 5 minut →
es,every minute} [--filters FILTERS] , - creates new policy.

Example :

# python elasticsearch_admin.py elect-create-policy --path "/ericsson/enm/dumps" →
 --log-retention "1 hour" --frequency "every 6 hours" --filters '{"severity":"in →
fo"}'

Policy created successfully at /opt/ericsson/elasticsearch/policies/export_logs_ →
every_6_hours_with_retention_1_hours_info.json
```

```
-elect-list-policies , - lists all available policies

Example :

# python elasticsearch_admin.py elect-list-policies
```

```
-elect-manage-policies [-h] [--disable-policy DISABLE_POLICY][--enable-policy EN →
ABLE_POLICY][--remove-policy REMOVE_POLICY], - Manage policies like remove or en →
able or disable policies

Example:

# python elasticsearch_admin.py elect-manage-policies --enable-policy export_log →
s_every_6_hours_with_retention_1_hours_neo4j.json

Selected policy export_logs_every_6_hours_with_retention_1_hours_neo4j enabled s →
uccessfully
```

```
# python elasticsearch_admin.py elect-manage-policies --disable-policy export_lo
gs_every_6_hours_with_retention_1_hours_neo4j.json

Selected policy export_logs_every_6_hours_with_retention_1_hours_neo4j disabled
successfully

# python elasticsearch_admin.py elect-manage-policies --remove-policy export_log
s_every_6_hours_with_retention_1_hours_neo4j.json
```

Following is the argument parser for option 11 in the Elasticsearch DBA tool menu:

```
[es_admin@ieatlms4906 elasticsearch]$ ./elasticsearch_admin.py export-logs-in-on
e-off --help
usage: elasticsearch_admin.py export-logs-in-one-off [-h] --path PATH
--frequency
{current-days-data,last-3-hours-data,last-1-hour-data,last-15-minutes-data,last-
5-minutes-data,last-1-minute-data}
[--filters FILTERS]

optional arguments:
-h, --help show this help message and exit
--path PATH Path to export logs
--frequency {current-days-data,last-3-hours-data,last-1-hour-data,last-15-minute
s-data,last-5-minutes-data,last-1-minute-data}
Capture data of following from index and export
--filters FILTERS Available filters 1.tag 2.severity 3.host 4.program
example:'{"severity":"info"}'

Example :

./elasticsearch_admin.py export-logs-in-one-off --path '/ericsson/enm/dumps' --f
requency last-5-minutes-data --filters '{"severity":"info"}'

To export logs from history indices :

[es_admin@ieatlms4906 elasticsearch]$ ./elasticsearch_admin.py export-log-histor
y-in-one-off --help
usage: elasticsearch_admin.py export-log-history-in-one-off
[-h] --index INDEX --path PATH [--filters FILTERS]

optional arguments:
-h, --help show this help message and exit
--index INDEX export data from given index
--path PATH Path to export logs
--filters FILTERS Available filters 1.tag 2.severity 3.host 4.program
example:'{"severity":"info"}'

Example :

./elasticsearch_admin.py export-log-history-in-one-off --index 'enm_logs-applica
tion-2020.07.10' --path '/ericsson/enm/dumps' --filters '{"severity":"info"}'
```

6.8 Configure ENM on Cloud Email Relay Service to Add Routing Notifications by Email

> Update ENM on Cloud Email Relay to route network notifications by email.

This procedure requires running a full upgrade for ENM on Cloud deployment. This procedure covers the use case where this change is applied by upgrading ENM on current software version.

Prerequisites

— Access to `keystonerc` file for the deployment.

— Identify the current installed version of ENM software deployment. Use all documentation relevant to installed software version.

— Access to Microsoft Office 2016 to use the ENM on Cloud Site Engineering Data (SED).

— Access to the VNF Lifecycle Management Upgrade Instructions.

— Access to the ENM on Cloud Upgrade Instructions.

— Access to a client machine to run openstack operations. On the Small Integrated ENM deployment, use the VMS as the client machine.

— Images belonging to current software baseline deployed are available in glance.

Steps

1. Retrieve the current ENM `sed.json` from VNF-LCM to client machine:

   Note: Log on to VNF-LCM services VM using the external IP address, `<external_ip_for_services_vm>`.

   — For access to VNF-LCM Non-HA deployments, replace `<external_ip_for_services_vm>` with the value defined for `<external_ipv4_for_services_vm>` or `<external_ipv6_for_services_vm>` fields in the VNF-LCM SED.

   — For access to VNF-LCM HA deployments, replace `<external_ip_for_services_vm>` with the value defined for `<external_ipv4_vip_for_services>` or `<external_ipv6_vip_for_services>` fields in the VNF-LCM SED.

2. Import an existing `sed.json` to the SED xls file.

   See the *How To* section in *Site Engineering Data for ENM on Cloud* for details.

   Note: Using a wrong SED version and Documentation artifact can lead to upgrade failure.

3. Update the `<EMAIL_DOMAIN>` field with new value needed for `Email Relay` and generate new `sed.json` file.

Note: Ensure that the new email relay value in the SED is correct, and ensure the value `EMAIL_DOMAIN=<new_email_domain_value>` is functional before starting an ENM upgrade.

4. Ensure that the only change between the old and new generated `sed.json` is for `email_domain` field:

```
[root@openstack-client ]# diff new-sed.json old-sed.json
```

Example:

```
[root@openstack-client ]# diff new-sed.json old-sed.json
14c14
< "EMAIL_DOMAIN":"new-ericsson.com",
---
> "EMAIL_DOMAIN":"old-ericsson.com",
```

5. Transfer the updated `sed.json` file to VNF-LCM. See *Updating ENM Deployment Workflows and Configuration* in *ENM on Cloud Upgrade Instructions*.

6. Follow all appropriate chapters in *ENM on Cloud Upgrade Instructions* for the ENM deployment type.

   Perform an end-to-end upgrade procedure, including all post install steps.

   — Skip the following chapters when executing *ENM on Cloud Upgrade Instructions*.

     These chapters are not applicable when using same software baseline.

     - Retrieve Required Artifacts for ENM on Customer Cloud
     - Upload Images to OpenStack for ENM on Customer Cloud
     - Upload Images to OpenStack for Small Integrated ENM Deployment

   — Skip all `workflow rpm` installation steps when executing *Updating ENM Deployment Workflows and Configuration*.

     There is no workflow change when upgrading to same software baseline.

   Note: If any failure is encountered during ENM upgrade procedure, or the `<new_email_domain_value>` is not working as expected, a rollback of ENM to the `<old_email_domain_value>` value may be required.

   Contact local Ericsson support for recommendation, else see *Rollback ENM on Cloud* in *ENM on Cloud Upgrade Instructions* to perform the ENM rollback.

Results

The email relay service is configured to forward email to the updated destination.

7 Application Maintenance Tasks

7.1 Flow Automation

Flow Automation (FA) is a new generic workflow-based framework and application which will allow **Flows** to be designed and executed. A **Flow** is an automated sequence of steps and operations to achieve an end-to-end goal.

Flows will be implemented as workflows based on the **OMG BPMN** standard. Flows will be designed using a combination of tools provided by the Flow Automation SDK and the Camunda Modeler visual designer.

The **Camunda BPM** 3PP will supply the workflow execution engine component. A rich set of BPMN features and workflow engine features are supported by Camunda BPM. Flow Automation will expose many of the BPMN and workflow engine features.

7.1.1 Housekeeping Job for Flow Automation

Housekeeping job is an internal flow within the Flow Automation application with the following characteristics and permissions. It allows for the following interactions with it.:

Characteristics:

- It is deployed and started when Flow Automation application is installed.
- It is configured to perform housekeeping every 24 hours (at midnight) to clean up data which are older than 7 days.
- There will be always one single instance running for this flow.
- It cannot be started, suspended, deleted, enabled/disabled, activated/deactivated or imported by administrator or any other operators.
- If any incidents happen with an instance of this flow, that instance will be removed and started again automatically by the flow automation application.

Capabilities and Roles:

Only users with the following capabilities are able to interact through the user task with this flow:

Application	Resource	Operation	Description
Flow Automation	flowautomation	remove	Allows the removal of existing flows from the flowautomation application.

That includes users with the role: Flowautomation_Administrator.

Interactions:

The way to interact with the flow is through the recurring associated user task presented to user every minute.

The Administrator or user with the above capabilities sees the current running instance of this flow from the Flow Instance details page, and is sees a User Task named "Flow Automation House Keeping Job". That task allows them to request an immediate housekeeping without having to wait until midnight. This execution performs housekeeping immediately, and cleans up data which is older than 7 days.

7.2 Post Deployment Procedure for Ericsson Expert Analytics (EEA) Integration

Use this procedure to configure a physical ENM deployment to provide launcher links for the EEA application.

Prerequisites

— Root access to ENM to allow configuration

— A good understanding of Linux administration

— Access to the EEA installation and the required configuration parameters

Steps

1. Log on to the ENM MS as the `litp-admin` user, then switch to the `root` user. :

   If password authentication is disabled for the litp-admin user, then refer to *Log on to the MS When Password Authentication is Disabled* in the *LITP Node Hardening Instructions*.

   ```
   # ssh litp-admin@<management_vm_ip>
   # su -
   ```

   or in the case of Cloud deployment, log on to HTTP VM :

   ```
   >ssh -i <privatekey> cloud-user@<httpd_vm_ip>
   ```

2. Execute this command at the shell command prompt:

```
EEA_INTEGRATION_FOLDER=/ericsson/tor/data/eea_integration
```

3. Add PIB hostname property to the Presentation web host:

```
> cd /ericsson/pib-scripts/etc
> ./config.py update --name=PresentationService_webHost --service_identifier →
=presentation-server
--app_server_address svc-2-presentation:8080
--value=default:<web_host_default>,eea_hostname:<hostname>
```

   Default hostname (*<web_host_default>*) can be found in `global.properties` file of the environment.

4. Execute following commands to set proper permissions for files, that will be available to *<jboss_user>*:

```
> EEA_INTEGRATION_FOLDER=/ericsson/tor/data/eea_integration
> chown -R jboss_user:jboss ${EEA_INTEGRATION_FOLDER}
> chmod -R 770 ${EEA_INTEGRATION_FOLDER}
```

5. Copy UI files, that allow the presentation server to display the links on ENM Launcher page:

```
> cd ${EEA_INTEGRATION_FOLDER}/apps
> cp -rp ./* /ericsson/tor/data/apps
```

7.3 Neo4j DPS Administration Utility

A general information/administration script is available on the host where Neo4j service is running. This can be used as a troubleshooting/general information utility.

Note: The only authorized ways for administering, monitoring or troubleshooting Neo4j is by using the DPS Database Admin Utility, ENM Neo4j Troubleshooting Guide, or procedures defined therein. Access to the Neo4j Database via direct "CYPHER" commands is strictly prohibited, and may result in unrecoverable corruption or data loss. Usage of other features or methods to run any operations, monitoring, or activities on data managed by the Neo4j Service is prohibited. If there are any features needed that are not provided and documented herein then contact Ericsson Support.

— The Neo4j Admin Tool `<dps_db_admin.py>` must be used exclusively and directly by ENM System Administrators to support Admin Activity.

— Do not execute the Neo4j Admin tool as part of any scheduled, automated or crontab activity. This is because such activity is not validated and has an impact on resource usage.

Prerequisites

— A command window is open and you have logged in with root user:

Table 23 Utility Options

	Script Option	Description
1	Neo4j Version	Displays the version of Neo4j installed.
2	Neo4j Service Uptime	Displays how long the Neo4j service has been running.
3	Neo4j File System	Displays a summary of Neo4j filesystem.
4	Graph Metadata	Displays Neo4j graph metadata.
5	Active Neo4j Configurations	Displays active Neo4j configurations.
6	List Longest Currently Running queries	List top 20 longest running queries at the time of command execution.
7	Neo4j Log	Displays warnings and errors from the neo4j log file: 1. Neo4j Warning Logs 2. Neo4j Error Logs
8	Cluster Overview	Displays general information about the cluster.
9	Clean Neo4j Heap Dumps	Gives new heap dumps a timestamp and removes the second oldest heap dump if there are more than two.
10	Switch HA Groups from Neo4j Active System	Switching active Postgresql, Elasticsearch, JMS, MySql HA groups from Neo4j active node. **Note:** Only db-2 on Extra Large ENM environment can perform switch.
11	Verify Neo4j Filesystem Threshold Value	Verifies the threshold value for the filesystem.
12	Generate Troubleshooting Report	Provides interactive interface to collect necessary data, such as logs and thread dumps, for troubleshooting reports.
13	Replication Lag Report	Provides current lag data for server, refreshing every 5 seconds.
14	Troubleshooting Toolkit	Options available in Troubleshooting Toolkit:

<table>
<tr><th></th><th>Script Option</th><th>Description</th></tr>
<tr><td></td><td></td><td>Table 24
<table>
<tr><td>1</td><td>Restart a Neo4j instance</td><td>Restarts an instance of Neo4j on a specified database node.</td></tr>
<tr><td>2</td><td>Unbind and Restart Instances</td><td>Restart Neo4j instances and unbind each one of them. If --db is not provided, all instances will be unbound and restarted.</td></tr>
<tr><td>3</td><td>Store Copy Recovery</td><td>Allow Neo4j to run store copy by stopping the given Neo4j instance, removing its data, and starting it again.</td></tr>
<tr><td>4</td><td>Seed Cluster</td><td>The graph.db of the specified healthy --db will be copied to the other instances of Neo4j cluster and the cluster will be restarted.</td></tr>
<tr><td>5</td><td>Errors overview</td><td>Display an overview of recent Neo4j errors.</td></tr>
<tr><td>6</td><td>Healthcheck Disable/Enable</td><td>Disable or enable the healthcheck.</td></tr>
</table></td></tr>
<tr><td>15</td><td>Clean Neo4j Label Scan Store File</td><td>Clear all data contained in the label scan store.</td></tr>
</table>

Steps

1. Run the following command:

```
/opt/ericsson/neo4j/util/dps_db_admin.py
```

Example

```
root@db-1 ~]# /opt/ericsson/neo4j/util/dps_db_admin.py
********************************************************************************
                            DPS DB ADMIN UTILITY
********************************************************************************
         Select the action you want to perform:
         1. Neo4j Version
         2. Neo4j Service Uptime
         3. Neo4j File System
         4. Graph Metadata
         5. Active Neo4j Configurations
         6. List Longest Currently Running queries
         7. Neo4j Log
         8. Cluster Overview
         9. Clean Neo4j Heap Dumps
         10. Switch HA Groups from Neo4j Active System
         11. Verify Neo4j Filesystem Threshold Value
         12. Generate Troubleshooting Report
```

```
        13. Replication Lag Report
        14. Troubleshooting Toolkit
        15. Clean Neo4j Label Scan Store File
        0.  Quit

    Enter your choice in digits:
```

7.4 Disable Hardware Acceleration in Firefox

This task should only be performed if you are using Firefox running on a windows operating system. There is a known memory leak with that configuration. This task outlines the temporary workaround to resolve that memory leak issue.

Note: This task may reduce application performance and must only be completed when memory leak has been confirmed.

Steps

1. Click the **Menu** icon on the top-right of the Firefox browser.
2. Click the **Options** icon on the menu dropdown.
3. Click **Advanced** tab on the options page.
4. Uncheck Use hardware acceleration when available.
5. Restart Firefox.

Results

Firefox will no longer continuously consume memory on affected environments.

7.5 Post Deployment Procedure to Enable Access to SON OM via ENM Application Launcher

Use this procedure to configure a physical Ericsson Network Manager (ENM) deployment to provide launcher links and Single Sign On (SSO) integration for the SON Optimization Manager (SON OM) product.

Prerequisites

— Root access to ENM to allow configuration

— Good understanding of Linux administration

— Access to the SON OM installation and know the required configuration parameters

Use the following steps to configure integration of SON OM Single Sign On (SSO) from ENM deployment.

Steps

1. Log on to the ENM MS as the `litp-admin` user, then switch to the `root` user for physical deployments. In case of Cloud deployment, log on to `httpd` VM.
2. Execute following command on shell.

   ```
   SONOM_INTEGRATION_FOLDER=/ericsson/tor/data/sonom_integration
   ```

3. Create `deployment.properties` file and copy to `SONOM_INTEGRATION_FOLDER` location.

   Use the following information to create the file contents.

Property	Description	Valid Values	Sample Value
sonom_hostname	IP address or host name of SON OM portal deployed	IPv4 or IPv6 address	10.45.19.25
sonom_port	HTTP port number used by Citrix StoreFront, if used value 443, `was_citrix_protocol` has to be set to HTTPS if used value 80, `was_citrix_protocol` has to be set to HTTP	443 or 80	433
sonom_protocol	HTTP protocol used by SON OM	HTTPS or HTTP	HTTPS
sonom_sso	Enable or disable SON OM SSO from ENM. 'true' to enable SON OM SSO 'false' to disable SON OM SSO Reference document for configuration on SON OM: SON OM Interwork Description for ENM,	true/false	true

Property	Description	Valid Values	Sample Value
	2/15519-CXP 902 1735/19 Uen		

Sample `deployment.properties` file contents:

```
sonom_hostname=10.45.19.25
sonom_port=443
sonom_protocol=http
sonom_sso=true
```

4. Execute following commands to set proper permissions for files, that will be available to `jboss_user`.

```
SONOM_INTEGRATION_FOLDER=/ericsson/tor/data/sonom_integration
chown -R jboss_user:jboss ${SONOM_INTEGRATION_FOLDER}
chmod -R 770 ${SONOM_INTEGRATION_FOLDER}
```

5. Copy UI files, that will allow the presentation server to display the links on ENM Launcher page.

```
cd ${SONOM_INTEGRATION_FOLDER}/apps
cp -rp ./* /ericsson/tor/data/apps
```

7.6 Post Deployment Procedure to Enable Access to Business Objects and Network Analytics Server via ENM Application Launcher

Note: WAS refers to OCS (OSS Client Solution) deployment in ENIQ.

Use this procedure to configure a physical Ericsson Network Manager (ENM) deployment to provide launcher links and Single Sign On (SSO) integration for the Ericsson Network IQ Statistics(ENIQ-S) Business Objects(BO) and Network Analytics (NetAn) products.

Prerequisites

— Admin group permissions to ENM LMS to allow configuration.

— A good understanding of Linux administration.

— Have previously performed the steps in *SSO Configuration for OCS AD DS Server* of SSO Configuration for Network Analytics Server and Ericsson Business Intelligence Deployment System Administrator Guide, 1543-CNA 403 2826.

— Access to BO and Network Analytics Server credentials to obtain the necessary configuration parameters.

The procedure creates two files `deployment.properties` and `enm_ca.jks`, storing them in `/ericsson/tor/data/eniq_was_integration` folder for the services to recognize the integration and reconfigure itself.

Configuration of ENIQ-S integration:

Steps

1. Log on to the ENM MS as the `litp-admin` user, then switch to the `root` user for physical deployments. If a cloud deployment, log on to `httpd` VM.
2. Export `ENM_External_Entity_CA` certificate chain and store it in `ENM_External_Entity_CA.JKS` file in `/ericsson/tor/data/eniq_was_integration` folder on SFS share:
    a. Log on to ENM Launcher, and from the Provisioning section, select **`Command Line Interface`**.
    b. Execute CLI Command, making sure that password is empty:

    ```
    pkiadm certmgmt CACert --exportcert --entityname ENM_External_Entit →
    y_CA --format JKS
    ```

    c. Save the file to local disk, renaming the file to `enm_ca.jks` (all lowercase).
    d. Transfer the file to ENM Management Server, and copy it to the `/ericsson/tor/data/eniq_was_integration` folder.
3. Create `deployment.properties` file in `/ericsson/tor/data/eniq_was_integration` folder.

    Use the information given in the following table to create the file contents.

Property	Description	Valid Values	Sample Value
`was_citrix_protocol`	Http protocol used by Citrix StoreFront	https or http	https
`was_citrix_port`	Http port number used by Citrix StoreFront, if used value 443, was_citrix_protocol has to be set to https if used value 80, was_citrix_proto	443 or 80	433

Property	Description	Valid Values	Sample Value
	col has to be set to http		
`was_citrix_hostname`	IP address of Citrix Hostname	IPv4 address	10.95.19.25
`was_ad_ldap_username`	Microsoft Active Directory account user name used to communicate through Lightweight Directory Access Protocol (LDAP). This account requires to be in "Domain Administrators" AD group, to update users' passwords and status	Microsoft Active Directory account user name used to communicate through Lightweight Directory Access Protocol (LDAP). This account requires to be in "Domain Administrators" AD group, to update users' passwords and status	`CN=<enmldap>`
`was_ad_ldap_password`	AD account password, used to communicate through LDAP over Secure Socket Layer (SSL)	String	`Abc@123`
`was_ad_ldap_fqdn`	AD LDAP Fully Qualified Domain Name	String, made from was_ad_ldap_basedn, made by removing occurrences of "DC=" and replacing "," with "."	`activedirectoryserver.domain.com`
`was_ad_ldap_basedn`	AD LDAP Base Domain Name	String, in format accepted by LDAP, representing Base Domain name	`DC=<activedirectoryserver>,DC=<domain>,DC=<com>`
`was_ad_hostname`	IP address of Microsoft Active Directory (AD) Hostname	IPv4 address	10.95.19.24

Property	Description	Valid Values	Sample Value
`was_ad_domain_name`	Microsoft Active Directory domain name	String containing only characters and numbers	ADDOMAIN1
`netan_sso`	Enables or disables SSO for Network Analytics Server applications. If SSO is enabled (true) on ENM for Network Analytics Server, SSO must be enabled on Network Analytics Server. Reference document for SSO Configuration for OCS AD DS Server, System Administrator Guide, 1543-CNA 403 2826	true or false	true
`netan_protocol`	HTTP protocol used by Network Analytics Server Web Player Note: This parameter is required for configuring Network Analytics Server Web Player	`HTTPS`	`HTTPS`
`netan_port`	Https port number used by Network Analytics Server Web Player. if used value 443, netan_protocol has to be set to https	443	443

Property	Description	Valid Values	Sample Value
	Note: This parameter is required for configuring Network Analytics Server Web Player		
netan_hostname	IP address of Network Analytics Server Web Player Note: This parameter is required for configuring Network Analytics Server Web Player	IPv4 address	10.95.19.5
bo_sso	Enables or disables SSO for BO applications If SSO is enabled (true) on ENM, SSO must be enabled on BO. Reference document for SSO Configuration for OCS AD DS Server, System Administrator Guide, 1543-CNA 403 2826	true or false	true
bo_protocol	HTTP protocol used by BO Note: This parameter is required for configuring BO Web Applications	HTTPS or HTTP	HTTP
bo_port	HTTP port number used by BO Web Applications:	8443 or 8080	8443

Property	Description	Valid Values	Sample Value
	Central Management Console (CMC) and BILaunchPad, if used value 8443, `bo_protocol` has to be set to HTTPS if used value 8080, `bo_protocol` has to be set to HTTP Note: This parameter is required for configuring BO Web Applications		
`bo_hostname`	IP address of BO Web Applications	IPv4 address	10.95.19.2

Sample `deployment.properties` file contents:

```
was_citrix_hostname=10.95.19.25
was_citrix_port=443
was_citrix_protocol=https
was_ad_hostname=10.95.19.24
was_ad_domain_name=ADDOMAIN1
was_ad_ldap_username=CN=enmldap
was_ad_ldap_password=Abc@123
was_ad_ldap_basedn=DC=activedirectoryserver,DC=domain,DC=com
was_ad_ldap_fqdn=activedirectoryserver.domain.com
bo_hostname=10.95.19.2
bo_port=8443
bo_protocol=https
bo_sso=false
netan_hostname=10.95.19.5
netan_port=443
netan_protocol=https
netan_sso=false
```

Note: If the Customer does not have either `NetAn` or `BO`, the default values specified in the sample `deployment.properties` file above should be used.

Please run **`dos2unix`** on the `deployment.properties` file after changing it.

4. Execute following commands to set permissions for files to `jboss_user`:

```
INTEGRATION_FOLDER=/ericsson/tor/data/eniq_was_integration
chown -R jboss_user:jboss ${INTEGRATION_FOLDER}
chmod -R 770 ${INTEGRATION_FOLDER}
```

5. Copy application user interface configuration files:

   This allows the presentation server to display the links on ENM Launcher page.

```
cd ${INTEGRATION_FOLDER}/apps
cp -rp ./* /ericsson/tor/data/apps
```

7.7 Minimize Data Loss

> The following describes how to use the minimize data loss solution in ENM. Minimize data loss is an optional solution providing data protection. It is installed as part of the ENM scripting service during ENM deployment.

Minimize data loss ensures data protection for the following functional data:

— User supplied configuration data used by ENM Fault Configuration Security (FCAPS) applications, such as the following examples:

  — Parameters in the Network Element MO - `networkElementId`, `neType`, `platformType`, and so on

  — Parameters in the Connectivity Information MO – `ipAddress`, `Port`, and so on

You can integrate minimize data loss with ENM system-level functions for the restore and rollback procedures. ENM schedules system-level backup snapshots at certain times (daily, weekly, bi-weekly, before upgrade, and so on), whereas network topology data is in constant flux, therefore an unquantifiable level of this network topology data may be lost. The impact is governed by the time interval between the decision to rollback and restore and the time-stamp of the point-in-time backup used. The minimize data loss solution can help reduce that time interval. This way, you can schedule more frequent network topology data exports and perform export/import of network topology data on demand.

Note: If any Certificate related operations are performed between the DB backup and restore activities, the data of such operations like Entity Info and Certificates data etc., will be lost. This may cause issues like connection or sync failures with Nodes and Node Certificate enrollment failures. To avoid such issues, manually issue the Certificates for the Nodes that are re-added during the Minimize Data Loss procedure.

The following tasks are detailed in this section:

1. User Setup on page 257
2. Enable Scheduled Network Topology Data Exports on page 257
3. Manually Export Data on page 258
4. Manually Import Data on page 260
5. Disable Scheduled Network Topology Data Exports on page 259

Note: PM Subscription is currently not supported in this solution.

7.7.1 User Setup

To use the minimize data loss solution create an ENM user that has both `Scripting_Operator` and `Cmedit_Administrator` rights. Once this is complete, export or import the network topology data on demand. Refer to *Managing Roles* in page 354 for more information.

Prerequisites

You have ENM administrative roles, such as create user and assign rights.

Steps

1. Launch the ENM User Management Interface.
2. Log on as an ENM administrative privilege user.
3. Create an ENM user that is assigned the following rights:
   - `Scripting_Operator`
   - `Cmedit_Administrator`
4. Log off ENM User Management.

Results

You have created a predefined ENM user to apply the minimize data loss solution.

7.7.2 Enable Scheduled Network Topology Data Exports

This task allows you to enable scheduled network topology exports and set preferred export scheduling policies and intervals.

Prerequisites

— User has `Scripting_Operator` rights.

— User has `Cmedit_Administrator` rights.

Steps

1. As the `<predefined-user>` with the Scripting_Operator and Cmedit_Administrator roles, login to ENM Launcher and select Shell Terminal on Scripting link.
2. As the `<predefined-user>` execute the `setup.py` script and follow prompts.

```
[scp-1-scripting~] $ cd /opt/ericsson/criticalbackup/bin/
    [scp-1-scripting~] $ ./setup.py
```

Note: Make sure you use the same password as in step 1 because password validation against the LDAP/PAM does not take place during step 2.

3. Log off from General Scripting VM.

   The generated cron job becomes active after 30 minutes.

Results

Scheduled network topology data export is enabled. At configured intervals, generated network-topology export files are stored in the `/ericsson/tor/no_rollback/criticalbackup/cron_backups/` directory in the ENM system.

After This Task

For more information on scheduling policies refer to *Schedule Execution of User Scripts via Cron Service* in the page 354.

7.7.3 Manually Export Data

This task explains how to manually perform network topology data export.

Prerequisites

— User has `Scripting_Operator` rights.

— User has `Cmedit_Administrator` rights.

— The location to store the exported Network topology data has sufficient space available.

Steps

1. As the `<predefined-user>` with the Scripting_Operator and Cmedit_Administrator roles, login to ENM Launcher and select Shell Terminal on Scripting link.
2. Export the network topology data.

   ```
   python /opt/ericsson/criticalbackup/export_ne_topology.py -o nodes.jsonlines
   ```

3. Log off ENM General Scripting VM.

Results

Network topology data is exported and stored in the path provided by the argument `-o/--output` in Step 2. If just a file name is provided for the argument `-o/--option` in Step 2, then the file containing the Network topology data will be created in the directory from which the script is run.

7.7.3.1 Constraints on data when using the network topology export feature

- The supported file type extension is `.jsonlines` .
- The full directory path to the file must exist.
- If a file name only is supplied, the file is created in the current working directory.
- If the file already exists, please supply the `-f` argument to overwrite it. Otherwise, an error will be returned.
- The file is created with read-only permissions.
- Metadata (such as duration of export, number of Managed Objects exported) will be:
  - Printed to the user (if the `-v` argument is supplied).
  - Written to the top of the export file.
  - Written to a separate file with the same name as the export file but with the `.metadata` extension.

7.7.4 Disable Scheduled Network Topology Data Exports

This task allows for temporary or permanent disabling of scheduled network topology exports. Optionally, this task can be done as part of the ENM rollback or restore procedures workflow. Refer to *ENM Backup and Restore Workflow* in *ENM OMBS System Administrators Guide* for more information.

Prerequisites

— User has `Scripting_Operator` rights.

— User has `Cmedit_Administrator` rights.

— Scheduled network topology data export is enabled.

Steps

1. As the `<predefined-user>` with the Scripting_Operator and Cmedit_Administrator roles, login to ENM Launcher and select Shell Terminal on Scripting link.
2. As `<predefined-user>`, remove the cron job for the critical backup from the <predefined-user> cron:

   ```
   [scp-1-scripting~] $ crontab -e
   ```

   An example of the critical backup cron job is the following:

   ```
   0 2 * * * /opt/ericsson/criticalbackup/crontabs/cron.sh 2>/dev/null
   ```

3. Log off from ENM General Scripting VM.

Results

Scheduled export jobs stop executing on ENM General Scripting VM.

7.7.5 Manually Import Data

This task explains how to manually perform network topology data import. Optionally, this task can be done following recent, successful ENM rollback or restore procedures.

Prerequisites

— User has `Scripting_Operator` rights.

— User has Cmedit_Administrator rights.

— There is at least one previously created network topology data export file. For scheduled exports, the file is located in the `/ericsson/tor/no_rollback/criticalbackup/cron_backups/` directory. For manual exports, the file is located in user home directory.

Steps

1. As the `<predefined-user>` with the Scripting_Operator and Cmedit_Administrator roles, login to ENM Launcher and select Shell Terminal on Scripting link.
2. Import the network topology data by running the following command:

   ```
   <predefined-user> $ python /opt/ericsson/criticalbackup/import_ne_topology.p
   y -i <full path to the network topology export file>
   ```

   Sample output for the import command is as follows:

   ```
   Name: Import NE Topology
   Start time: 2016-10-13 13:04:41
   End time: 2016-10-13 13:05:34
   Duration: 0:00:53
   Created NEs: 4 (LTE07dg2ERBS00001, LTE07dg2ERBS00002, LTE07dg2ERBS00003, LTE
   07dg2ERBS00004)
   Deleted NEs: 1 ( LTE07dg2ERBS00005)
   Failed to create: 1 (LTE07dg2ERBS00006)
   Failed to delete: 1 (LTE07dg2ERBS00007)
   Other failures: 0
   Import NE Topology complete Metadata file created at: samples/exp_2016-10-13
   T13:05:34.metadata
   ```

   The import process generates a detailed `Metadata` summary file. Import Output on page 262 details the output from the import command, and their associated actions.
3. Log off the ENM General Scripting VM when complete.

Results

Previously exported network configuration data is reapplied to the system.

Note: During a network topology data import errors can occur due to invalid attribute values (error no. 1009) or if the attributes are now mandatory (error no. 1005).

A re-import with a modification of the network topology data import file (.jsonlines), where the attributes are changed to valid values or the attributes are correctly populated after becoming mandatory, resolves this in certain cases. See limitations below:

Limitations:

- The re-import is feasible only for previously nonexistent NetworkElements, It does not work for existing NetworkElements in the system.
- The re-import will work only if the invalid attribute value is on the NetworkElement Managed Object (MO) itself. It will not work if it is an attribute on a NetworkElement child MO.

7.7.5.1 Import Output

Table 25 Import Output

Output	Actions	For more information refer to ENM Help
`Failed to delete`	Manually delete the nodes	*#help/app/cliapp/topic/tutorials_cm/DeleteNode*
`Failed to create`	Manually create nodes.	*#help/app/cliapp/topic/tutorials_cm/AddNode*
`Deleted NEs`	Manually remove residual information for nodes.	*#help/app/cliapp/concept/tutorials_pkiadm/Revocation_Management/RevokeCACertificate* and *#help/app/cliapp/concept/tutorials_pm/SetPmFunction*
`Created NEs`	Manually create PM Subscriptions and Certificates for nodes.	*#help/app/cliapp/concept/tutorials_pkiadm/Certificate_Management/ReissueCACertificate* and *#help/app/cliapp/concept/tutorials_pm/SetPmFunction*

7.8 ENM Launcher Administration Tasks

> This section contains the routine operation and maintenance tasks related to the administration of the ENM Launcher.

7.8.1 Update ENM Host Name

This task explains how to update the ENM hostname property that is shown on Launcher top bar.

This should be done by a system administrator when is required to change the ENM host name displayed in Launcher Top Bar.

For details on how to view and modify parameters using Platform Integration Bridge (PIB), refer to section Configuring PIB Parameters.

Note: Service name is `uiserv`

name	service_identifier	scope	Description	Default Value
`enmHostName`	`presentation-server`	`SERVICE`	Parameter to configure ENM host name	`enmHostName`

Result

The new ENM host name is displayed in the top bar on Launcher. Verify the parameter has changed using the read command.

7.8.2 Configuration of Clickable Links on Successful Logon

Potential Security Risk

This feature requires "`root`" access and that poses a Security Risk that customer has to accept. If such risk cannot be accepted, we strongly recommend that feature is not used

On successful logon, a list of custom links and information (free text) can be shown. This can be achieved by creating and filling a `linkList.txt` file in `/ericsson/tor/data/login/` folder. If the login folder is not present, must be created. If the file is empty or not present, nothing is shown.

Prerequisites

— Root access to servers is required.

Steps

1. Log on to each existing instance of HTTPD VM, then switch to the root user by following steps in Connect to a Virtual Machine on an ENM on Cloud Deployment on page 3
2. On the first HTTPD instance, create, if it does not already exist, the linkList.txt file in `/ericsson/tor/data/login/` directory. Create "login" directory if it does not alreadyexist:

   ```
   [root@svc-1-httpd]# mkdir -p /ericsson/tor/data/login
   [root@svc-1-httpd]# touch /ericsson/tor/data/login/linkList.txt
   ```

3. On the first HTTPD instance, put desired links or text messages in linkList.txt. On other HTTPD instances , check that the file contains the desired links or text messages. Use the following rules when updating the file:

   a. Each line can represent either a single link or a free text.

   b. In case of link, it is composed by two parts separated by comma: the first part indicates the link name that is shown on successful logon, the second part is the actual URL to point at.

   c. In case of free text, any combination of characters is allowed.

   d. Allowed protocols for links are http, https, ftp and sftp, invalid URLs are treated as a simple text line.

   e. White spaces in link names are permitted.

   f. Empty lines are ignored.

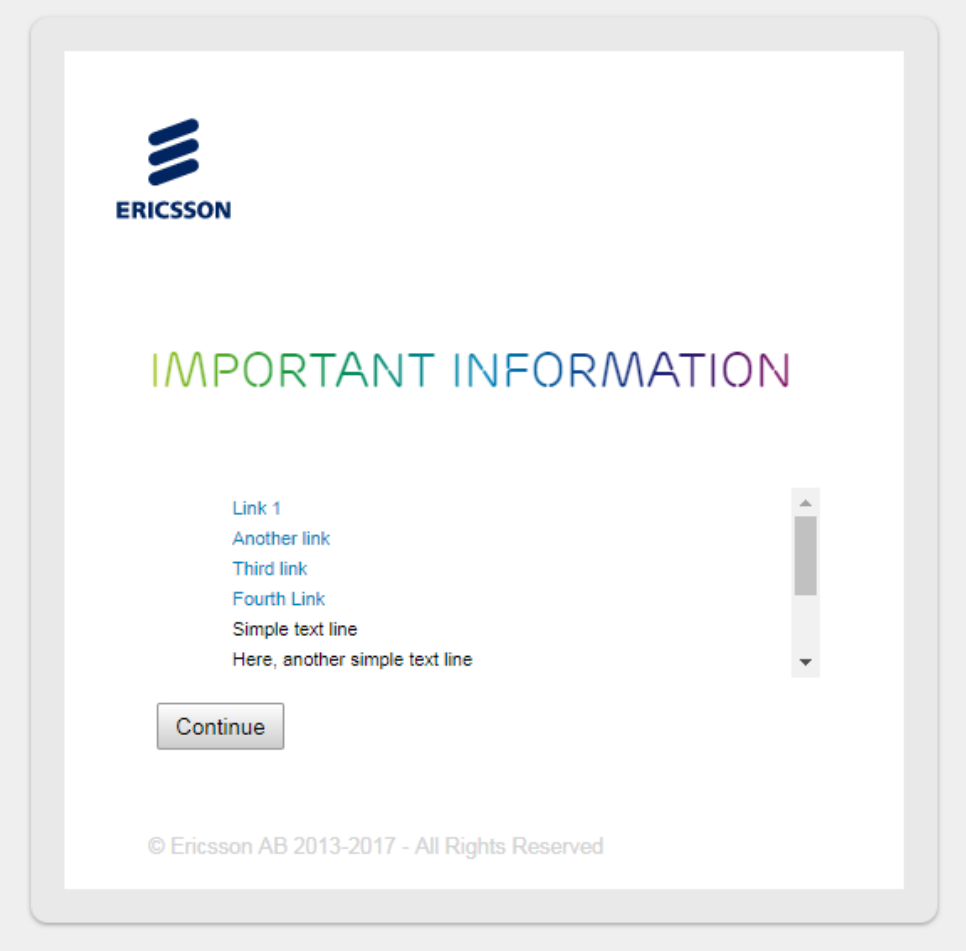
Example

Example of file:

```
Link 1 , https://en.wikipedia.org
Another link,http://ericsson.se
Third link ,http://localhost:8080/
Fourth Link, http://www.google.com
Simple text line

Here, another simple text line
```

Result:



4. Restart httpd-enm service on all HTTPD instances using the following command:

```
[root@svc-1-httpd]# service httpd-enm stop; service httpd-enm start
```

5. After restart of `httpd-enm` service on all HTTPD instances, the successful log on page shows the desired information messages.

Results

By creating and filling the `linkList.txt` file, the specified links and information are shown on the Successful Logon page.

7.8.3 Read a Specific Launcher Property

A particular Launcher property may need to be read to diagnose Launcher issues. This page explains how to read the properties stored.

For details on how to view and modify PIB parameters, refer to section Configuring PIB Parameters.

Note: Service name is `uiserv`

name	service_identifier	Description
`PresentationService_webHost`	`presentation-server`	Stores the web server to use for one or more web applications.
`PresentationService_webProtocol`	`presentation-server`	Stores the web protocol to use for one or more web applications.
`PresentatonService_webPort`	`presentation-server`	Stores the web port to use for one or more web applications.

The output is presented in the following Python Style format:

```
["ossMonitoringHost:172.16.30.19","eniqStatsHost:NOT_USED","alexHost:NOT_USED","default:enmapache.athtem.eei.ericsson.se","eniqEventsHost:NOT_USED","eniqBusinessHost:NOT_USED","eniqManagement:NOT_USED"]
```

The output contains comma-separated, key/value-paired properties that relate to the properties in the `/ericsson/tor/data/global.properties` file as this is where they are read from.

Result

You can see the requested host properties used by the Launcher.

7.8.4 Configure the Log In Legal Notice Message

On the log in page a legal notice message is prompted that have to be acknowledged before logging in. The default message is:

"

IF YOU ARE NOT AN AUTHORIZED USER STOP ANY ACTIVITY

YOU ARE PERFORMING ON THIS SYSTEM AND EXIT IMMEDIATELY.

This system is provided for authorized and official use only.

The usage of this system is monitored and audited.

Unauthorized or improper usage may result in disciplinary actions, civil or criminal penalties.

This system processes sensitive personal data.

The misuse of such data may generate considerable harm to the data subjects.

Be reminded of the confidentiality obligations you have when accessing this kind of data and the disciplinary consequences of improper handling.

"

This message can be customized by creating the `legalNotice.txt` file with desired message.

Prerequisites

Root access to servers is required.

Steps

1. Log on to each existing instance of HTTPD VM, then switch to the root user by following steps in Connect to a Virtual Machine on an ENM on Cloud Deployment on page 3
2. On the first HTTPD instance, create, if it does not already exist, the legalNotice.txt file in `/ericsson/tor/data/login/ directory`. Create "login" directory if it does not already exist:

   ```
   [root@svc-1-httpd]# mkdir -p /ericsson/tor/data/login
   [root@svc-1-httpd]# touch /ericsson/tor/data/login/legalNotice.txt
   ```

3. On the first HTTPD instance, put desired text message into created legalNotice.txt file. On other HTTPD instances , check that the file contains the desired text message.
4. Restart httpd-enm service on all HTTPD instances using the following command:

   ```
   [root@svc-1-httpd]# service httpd-enm stop; service httpd-enm start
   ```

5. After restart of `httpd-enm` service on all HTTPD instances, the log in page is presented with changed message.

Results

Creating the logalNotice.txt file, the legal notice message prompted on the Log In page is changed.

7.9 ENM ELEX CPI Library Maintenance Tasks

This chapter contains the routine operation and maintenance tasks related to the administration and availability of ENM ELEX CPI libraries.

7.9.1 Make CPI Libraries Available from ENM Launcher

This task describes how a system administrator makes a CPI library available in the ENM Launcher from **Documentation** > **Elex Library (ELEX)**. This procedure also enables the Alarm Monitor application to access alarm Operational Instructions (OPIs) documents contained in the ENM and in the Node CPI libraries.

To maintain the `elex` filesystem in working order ensure the filesystem space usage does not exceed 80%.

Before transferring a new CPI Library to the `elex` filesystem, check the size of the new CPI library, remove old CPI libraries, and ensure there is sufficient space for the new CPI library.

Note:
- The ENM CPI library provides OPIs for both for `ALARM` records and `ERROR_MESSAGEs` generated by ENM.
- The Node CPI libraries normally only include OPIs for `ALARM` records and not for `ERROR_MESSAGE` records.
- The Node CPI libraries also include OPIs for the alarms and `TRX MANUALLY LOCKED` generated by FMX. If the Node CPI does not contain them, it is not possible to launch the OPI from the Alarm Monitor.

Prerequisites

- For physical deployments: connect to the ENM Management Server (MS) as the litp-admin user and switch to the root user.
- For Cloud deployments follow Connect to a Virtual Machine on an ENM on Cloud Deployment on page 3, in order to log on to the 'httpd' Virtual Machine (VM).

Steps

1. Check the size of the new CPI library (`.alx` file) to be made available from the ENM Launcher.
2. Check the space available on the `elex` filesystem.

   ```
   # df -h /ericsson/enm/alex
   ```

   Example

   ```
   # df -h /ericsson/enm/alex
   Filesystem            Size  Used Avail Use% Mounted on
   <NAS ip address>:/vx/ENM404-alex
                         10G  373M  9.1G   4% /ericsson/enm/alex
   ```

   Ensure that the `elex` filesystem usage will not exceed 80% when the new CPI library is added to the filesystem.
3. Check the contents of the `/ericsson/enm/alex/libraries` directory and remove any old libraries.

   Example

   ```
   # ls -l /ericsson/enm/alex/libraries/
   -r-xr-xr-x. 1 root testers  57966471 May 26 15:05 lzn_7030205r43a.alx
   -r-xr-xr-x. 1 root testers 103413437 May 26 15:00 lzn7030205r44a.alx
   # rm lzn_7030205r43a.alx
   ```
4. Transfer the new CPI library to the `/ericsson/enm/alex/libraries` directory using SFTP.
5. Apply the required permissions (`r-r--r--`) to the `.alx` file.

   Example

   ```
   # cd /ericsson/enm/alex/libraries
   # chmod 444 lzn7030205r45a.alx
   ```
6. Verify that the `.alx` file has required permissions.
7. Verify that it is possible to view the new CPI library in the ENM Launcher from **Documentation** > **Elex Library (ELEX)**.

   ```
   # ls -l lzn7030205r45a.alx
   -r-xr-xr-x. 1 root root 103426610 May 25 15:55 lzn7030205r45a.alx
   ```
8. Run the `fmedit create` ENM CLI command to allow Alarm Monitor to access the OPIs contained in the CPI libraries stored in the `/ericsson/enm/alex/libraries` directory.

   ```
   fmedit create name=AlarmCpiDetails targetType=<see description below>, [targ →
   etModelIdentity="<see description below>"], libraryName="<see description be →
   low>", [alarmsPageTitle="<see description below>"], release="<see descriptio →
   n below>", [componentName="<see description below>"]
   ```

Attribute	Description
`targetType`	This is used by ENM applications to identify a particular alarm source type.
`targetModelIdentity`	This is an optional attribute and can be specified when it is needed to distinguish between different node CPI versions.
`libraryName`	This is the Alex library name associated with the specified target type.
`alarmsPageTitle`	This is an optional attribute and must be used for managing Alex libraries if the operational instructions are boundled in a single document.
`release`	This is an optional attribute and must be used for launching correct OPIs when the specific revision is required.
`componentName`	This is an optional attribute and must be used for launching correct OPIs when the specific component is required.

See *Create AlarmCpiDetails* tutorial in `fmedit` command set of the ENM CLI online help.

7.10 OpenDJ Administration Tasks

It contains the routine operation and maintenance tasks related to the administration of OpenDJ.

7.10.1 OpenDJ Routine Operation Tasks

The system administrator performs routine operation and troubleshooting tasks related to the administration of the OpenDJ LDAP database.

Prerequisites

— Access to the DB node on a Physical environment. Refer to the Local Ericsson Support for the default password for the root user.

— Access to the OpenDJ VMs in an ENM on Cloud deployment.

Result

The system administrator can retrieve OpenDJ LDAP database related information.

7.10.1.1 OpenDJ Directory Structure and Utilities

Note: Changing the directories is not recommended as this can cause an unrecoverable error with OpenDJ.

On Physical Environment

OpenDJ is installed in the `/opt/opendj/` folder on the DB Nodes. This folder stores the OpenDJ backends, server configuration files, and non-user-modifiable files.

OpenDJ userRoot database (backend) is stored in the `/opt/opendj/db/` folder on the DB Nodes.

Generic OpenDJ utilities are installed in `/opt/opendj/bin/` folder on the DB Nodes.

On Cloud Environment

OpenDJ is installed in the `/ericsson/opendj/opendj/` folder on the OpenDJ VM. This folder stores the OpenDJ backend, server configuration files, and non-user-modifiable files.

OpenDJ userRoot database (backend) is stored in the `/ericsson/opendj/opendj/db/` folder on the OpenDJ VM.

Generic OpenDJ utilities are installed in `/ericsson/opendj/opendj/bin/` folder on the OpenDJ VM.

Change OpenDJ Passwords

Instructions on changing the passwords used by OpenDJ are available in the page 355, in the sections *How to Change Root Passwords for OpenDJ* and *How to Change SSO Password for OpenDJ*.

Note: Because of the existing Access Control implementation, this procedure must be avoided unless necessary and performed with caution.

7.10.1.2 OpenDJ logs location and description

On Physical Environment

OpenDJ logs are located in folders on the DB nodes and Management Server. Refer to OpenDJ Log Files in ENM - Physical on page 271

On Cloud Environment

OpenDJ logs are located in folders on the Opendj VM. Refer to OpenDJ Log Files in ENM - Cloud on page 271

For more information on gathering the OpenDJ logs, contact Ericsson Local Support.

For more information on OpenDJ and OpenDJ ldap schema, configuration and troubleshooting, check the Official OpenDJ documentation: https://backstage.forgerock.com/#!/docs/opendj/3

7.10.1.2.1 OpenDJ Log Files in ENM - Physical

Table 26 OpenDJ Log Files in ENM

Path	Log file names	Node / Server
/tmp/	All logs with names beginning with "opendj-"	DB-1 / DB-2
/var/log/opendj/	All logs	DB-1 / DB-2
/var/ericsson/log/opendj/	All logs	DB-1 / DB-2
/var/log/	messages	DB-1 / DB-2
/var/VRTSvcs/log/	engine_A.log	DB-1 / DB-2
/var/log/opendj/	All logs (folder and log exist only if reconciliation has been performed on the system)	MS
/var/log/	messages	MS

7.10.1.2.2 OpenDJ Log Files in ENM - Cloud

Table 27

Path	Log file names	VM / Server
/tmp/	All logs with names beginning with "opendj-"	Opendj VM
/var/log/opendj/	All logs	Opendj VM
/var/log/opendj/server/	All logs	Opendj VM
/var/log/	messages	Opendj VM

7.10.1.3 List the Contents of the OpenDJ LDAP Database

Describes how to list the content of the OpenDJ LDAP Database.

Prerequisites

— Access to the DB node on a Physical deployment.

— Access to OpenDJ VMs in an ENM on Cloud deployment.

On Physical deployment, the path of the following commands is: `/opt/opendj/bin/`

On Cloud deployment, the path of the following commands is: `/ericsson/opendj/opendj/bin/`

Steps

1. To list items from the LDAP database use the ldapsearch command:

```
ldapsearch -p 1636 --useSSL --trustAll -D "cn=directory manager" -w ldap_pas →
sword -b "ou= ,dc= ,dc=com" objectClass=<filter>
```

   Main parameters:

```
-p = directory server port number, the default for ENM is 1636
--useSSL - use secure connection
--trustAll - automatically trust the certificates
-D = DN to use to bind to the server, the default for ENM is "cn=directory m →
anager"
-w = LDAP bind password - if omitted, you will be prompted for the password
-b = Base DN, i.e. "ou=people,dc=ieatclvmlms927-1,dc=com"
-h = hostname, if omitted, the search will be performed on the currently act →
ive host
objectclass=<filter> = this is used to define what information you can retri →
eve from LDAP, i.e. userType=enmUser
```

   For more parameters and detailed description of ldapsearch, visit https://backstage.forgerock.com/#!/docs/opendj/current/reference/admin-tools-ref#ldapsearch-1

Example 1

List all ENM users in the database (with details):

```
ldapsearch -p 1636 --useSSL --trustAll -D "cn=directory manager" -w ldap_passwor →
d -b "ou=people,$(grep COM_INF_LDAP_ROOT_SUFFIX /ericsson/tor/data/global.proper →
ties | cut -d '=' -f 2-)" userType=enmUser
```

List all ENM users in the database (user list):

```
ldapsearch -p 1636 --useSSL --trustAll -D "cn=directory manager" -w ldap_passwor →
d -b "ou=people,$(grep COM_INF_LDAP_ROOT_SUFFIX /ericsson/tor/data/global.proper →
ties | cut -d '=' -f 2-)" userType=enmUser | grep uid:
```

List all COM users in the database:

```
ldapsearch -p 1636 --useSSL --trustAll -D "cn=directory manager" -w ldap_passwor →
d -b "ou=groups,$(grep COM_INF_LDAP_ROOT_SUFFIX /ericsson/tor/data/global.proper →
ties | cut -d '=' -f 2-)" cn=com_users memberUid
```

List all M2M users in the database:

```
ldapsearch -p 1636 --useSSL --trustAll -D "cn=directory manager" -w ldap_passwor
d -b "ou=M2MUsers,$(grep COM_INF_LDAP_ROOT_SUFFIX /ericsson/tor/data/global.prop
erties | cut -d '=' -f 2-)" cn=* memberUid
```

List all AMOS users in the database:

```
ldapsearch -p 1636 --useSSL --trustAll -D "cn=directory manager" -w ldap_passwor
d -b "" cn=amos_users memberUid
```

List all positions in LDAP (with details):

```
ldapsearch -p 1636 --useSSL --trustAll -D "cn=directory manager" -w ldap_passwor
d -b "" objectclass=*
```

List all positions in LDAP (with details and operational attributes):

```
ldapsearch -p 1636 --useSSL --trustAll -D "cn=directory manager" -w ldap_passwor
d -b "" objectclass=* +
```

List all positions in LDAP (only the dn list):

```
ldapsearch -p 1636 --useSSL --trustAll -D "cn=directory manager" -w ldap_passwor
d -b "" objectclass=* dn
```

7.10.1.4 Check the Database (Backend) List

Describes how to check the backends used by OpenDJ.

Prerequisites

— Access to the DB node on a Physical deployment.

— Access to OpenDJ VMs in an ENM on Cloud deployment.

On Physical deployment, the path of the following commands is: `/opt/opendj/bin/`

On Cloud deployment, the path of the following commands is: `/ericsson/opendj/opendj/bin/`

Steps

1. To list all the backends used by OpenDJ, use the `dsconfig` command::

```
# dsconfig -h opendjhost0 -p 4444 -D "cn=directory manager" -w <password> --
trustAll -n --advanced list-backends

Backend        : Type        : enabled : base-dn                 : confident
iality-enabled

---------------:-------------:---------:-------------------------:----------
--------------
```

```
adminRoot      : ldif        : true    : cn=admin data           : -
ads-truststore : trust-store : true    : -                       : -
backup         : backup      : true    : -                       : -
monitor        : monitor     : true    : -                       : -
rootUser0      : ldif        : true    : cn=Directory Manager    : -
schema         : schema      : true    : -                       : -
tasks          : task        : true    : -                       : -
userRoot       : je          : true    : "dc=ieatlms4407,dc=com" : false
```

7.10.1.5 Check the OpenDJ Version, Database Status, Size and Details

Describes how to check the OpenDJ version, server status, server details, connection handlers, and data Sources.

Prerequisites

You have access to the DB node (on physical environment) or on opendj VM (on cloud environment).

7.10.1.5.1 For Physical environment

1. To check the OpenDJ version, server status, server details, connection handlers, and data Sources use the `status` command.

   The "`Version`" parameter shows information about the current OpenDJ version and used patches.

```
[root@ieatrcxb4363 bin]# /opt/opendj/bin/status --offline

>>>> General details

Version                                  : ForgeRock Directory Services 6. →
5.0

Installation and instance path  : /opt/opendj

Run status                               : Started

Host name                               : ieatrcxb4363

Administration port (LDAPS)   : 4444

>>>> Connection handlers

Name                    : Port : Protocol    : Security  : Status
------------------------:------:-------------:-----------:---------
HTTP                    : 8447 : HTTP        : SSL       : Enabled
JMX                     : 1689 : JMX         : SSL       : Enabled
LDAP Connection Handler : 1389 : LDAP        : Unsecured : Disabled
LDAPS                   : 1636 : LDAP        : SSL       : Enabled
LDIF Connection Handler : -    : LDIF        : -         : Disabled
```

```
Replication port        : 8989 : Replication : SSL       : Enabled

SNMP Connection Handler : 161  : SNMP        : -         : Disabled

>>>> Local backends

Base DN               : Backend   : Type : Status

----------------------:-----------:------:--------

cn=Directory Manager  : rootUser0 : LDIF : Enabled

dc=ieatlms4407,dc=com : userRoot  : DB   : Enabled


The tool is running in offline mode. Connect to the running instance in orde
r to have a more detailed status of the server
```

2. To check if OpenDJ is currently running use also the service opendj status command:

```
[root@ieatrcxb3211 litp-admin]# service opendj status
opendj (pid  3327) is running...
```

3. To check the OpenDJ service groups names, and their status (ONLINE, OFFLINE, PARTIAL, FAULTED), use the hagrp tool (as a root):

```
[root@ieatrcxb3211 litp-admin]# hagrp -state | grep opendj
Grp_CS_db_cluster_opendj_clustered_service        State                ieat
rcxb3028 |ONLINE|
Grp_CS_db_cluster_opendj_clustered_service        State                ieat
rcxb3211 |ONLINE|
```

4. To switch OpenDJ groups online and offline, use the following commands:

```
hagrp -offline Grp_CS_db_cluster_opendj_clustered_service -sys <db_hostname>
hagrp -online Grp_CS_db_cluster_opendj_clustered_service -sys <db_hostname>
```

   Replace `<db_hostname>` with the hostname of the DB node on which OpenDJ should be switched to offline of online state.

   Example

```
[root@ieatrcxb3211 litp-admin]# hagrp -online Grp_CS_db_cluster_opendj_clust
ered_service -sys ieatrcxb3211

[root@ieatrcxb3211 litp-admin]# hagrp -state | grep opendj
Grp_CS_db_cluster_opendj_clustered_service        State                ieat
rcxb3028 |ONLINE|
Grp_CS_db_cluster_opendj_clustered_service        State                ieat
rcxb3211 |ONLINE|
```

5. To check the OpenDJ backend (database) size use the df command, and to check the disk usage, use the du command. Both commands must be used on the database folder (`/opt/opendj/db/userRoot`):

```
[root@ieatrcxb3211 litp-admin]# df -h /opt/opendj/db/userRoot/
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vg_root-vg1_lv_root
                       15G  7.2G  6.8G  52% /

[root@ieatrcxb3211 litp-admin]# du -h /opt/opendj/db/userRoot/
```

```
3.1M    /opt/opendj/db/userRoot/
[root@ieatrcxb3211 litp-admin]#
```

7.10.1.5.2 For Cloud environment

1. To check the OpenDJ version, server status, server details, connection handlers, and data Sources use the `status` command.

   The "`Version`" parameter shows information about the current OpenDJ version and used patches.

```
[root@ieatenmc3a10-opendj-0 cloud-user]# /ericsson/opendj/opendj/bin/status --offline

>>>> General details

Version                                  : ForgeRock Directory Services 6.5.0

Installation and instance path  : /ericsson/opendj/opendj

Run status                               : Started

Host name                                : ieatenmc3a10-opendj-0

Administration port (LDAPS)   : 4444

>>>> Connection handlers

Name                    : Port : Protocol    : Security  : Status

------------------------:------:------------:-----------:---------

HTTP                    : 8447 : HTTP        : SSL       : Enabled

JMX                     : 1689 : JMX         : SSL       : Enabled

LDAP Connection Handler : 1389 : LDAP        : Unsecured : Disabled

LDAPS                   : 1636 : LDAP        : SSL       : Enabled

LDIF Connection Handler : -    : LDIF        : -         : Disabled

Replication port        : 8989 : Replication : SSL       : Enabled

SNMP Connection Handler : 161  : SNMP        : -         : Disabled

>>>> Local backends

Base DN               : Backend   : Type : Status

----------------------:-----------:------:--------

cn=Directory Manager  : rootUser0 : LDIF : Enabled

dc=ieatenmc3a10-9,dc=com : userRoot  : DB   : Enabled


The tool is running in offline mode. Connect to the running instance in order to have a more detailed status of the server
```

2. To check if OpenDJ is currently running use also the service opendj status command:

```
[root@opendj-1 /]# service opendj status
opendj (pid  10470) is running...
```

3. To check the OpenDJ service groups names, and their status (ONLINE, OFFLINE, PARTIAL, FAULTED), use the consul tool (as a root):

```
[root@opendj-1 /]# consul members | grep opendj
opendj-1                10.5.1.137:8301  alive   client  0.8.1  2         d →
c1
opendj-2                10.5.1.138:8301  alive   client  0.8.1  2         d →
c1
```

4. To check the OpenDJ backend (database) size use the df command, and to check the disk usage, use the du command. Both commands must be used on the database folder (`/opt/opendj/db/userRoot`):

```
[root@opendj-1 /]# df -h /ericsson/opendj/opendj/db/userRoot/
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/opendjvg-opendjvol
                      988M   48M  890M   6% /ericsson/opendj
[root@opendj-1 /]# du -h /ericsson/opendj/opendj/db/userRoot/
2.4M    /ericsson/opendj/opendj/db/userRoot/
```

7.10.1.6 Check the Replication Status

Describes how to check the status of the Replication between the two instances of OpenDJ.

Prerequisites

— On Physical Environment, you have access to the DB node.

— On Cloud Environment, you have access to OpenDJ VMs.

Steps

1. Go to directory `/opt/ericsson/com.ericsson.oss.security/idenmgmt/opendj/bin`.

2. Launch the `script monitor_replication.sh`:

```
./monitor_replication.sh

.....

ENM_OPENDJ: INFORMATION ( OPENDJ ): INFO: ..........monitor_replication.... →
..START

.........................

ENM_OPENDJ: INFORMATION ( OPENDJ ): INFO: ..........monitor_replication.... →
..OK: exit 0
```

See `/var/log/opendj/opendj-check-replication-opendj-<date/time>.log` for a detailed log of this operation.

7.10.1.7 Change the Replication Purge Delay Parameter

The replication purge delay is a property of the replication server specifying the period of time after which internal purge operations are performed on the replication changes database. Any change that is older than the purge delay is removed from the replication changes database, irrespective of whether that change has been applied. These steps can be performed as root or OpenDJ user, on any database node. The default Replication Purge Delay is three days.

Prerequisites

— Access to the DB node on a Physical deployment.

— Access to OpenDJ VMs in an ENM on Cloud deployment.

On Physical deployment, the path of the following commands is: `/opt/opendj/bin/`

On Cloud deployment, the path of the following commands is: `/ericsson/opendj/opendj/bin/`

Steps

1. Check the Replication Purge Delay for both OpenDJ instances

```
# dsconfig -h opendjhost0 -p 4444 -D "cn=directory manager" -w <password> -- →
trustAll -n \
  get-replication-server-prop \
  --provider-name "Multimaster Synchronization" --advanced \
  --property replication-purge-delay
Property                : Value(s)
------------------------:---------
replication-purge-delay : 3 d
```

```
# dsconfig -h opendjhost1 -p 4444 -D "cn=directory manager" -w <password> -- →
trustAll -n \
  get-replication-server-prop \
  --provider-name "Multimaster Synchronization" --advanced \
  --property replication-purge-delay
Property                : Value(s)
------------------------:---------
replication-purge-delay : 3 d
```

2. Change the Replication Purge Delay

   In this example, the Replication Purge Delay is changed to five days:

```
# dsconfig -h opendjhost0 -p 4444 -D "cn=directory manager" -w <password> -- →
trustAll -n \
  set-replication-server-prop \
  --provider-name "Multimaster Synchronization" --set replication-purge-dela →
y:5d
```

```
# dsconfig -h opendjhost1 -p 4444 -D "cn=directory manager" -w <password> -- →
trustAll -n \
  set-replication-server-prop \
```

```
  --provider-name "Multimaster Synchronization" --set replication-purge-dela
y:5d
```

3. Verify the changes

```
# dsconfig -h opendjhost0 -p 4444 -D "cn=directory manager" -w <password> --
trustAll -n \
  get-replication-server-prop \
  --provider-name "Multimaster Synchronization" --advanced \
  --property replication-purge-delay
Property                : Value(s)
------------------------:---------
replication-purge-delay : 5 d
```

```
# dsconfig -h opendjhost1 -p 4444 -D "cn=directory manager" -w <password> --
trustAll -n \
  get-replication-server-prop \
  --provider-name "Multimaster Synchronization" --advanced \
  --property replication-purge-delay
Property                : Value(s)
------------------------:---------
replication-purge-delay : 5 d
```

Results

Replication Purge Delay is changed.

7.10.1.8 OpenDJ Recovery when Replication Purge Delay is Exceeded

If one of the instances of OpenDJ is down for longer than the replication purge delay period (default is three days), the data from the replication changes database is lost and two OpenDJ instances are unsynchronized when the instance that was offline is brought back online. To check or change the replication purge delay follow the instructions in Change the Replication Purge Delay Parameter.

The replication purge delay is a property of the replication server specifying the time after which internal purge operations are performed on the replication changes database. Any change that is older than the purge delay period is removed from the replication changes database, irrespective of whether that change has been applied.

Prerequisites

— OpenDJ instances (after one of the instances was down longer than the replication purge delay) are not synchronized.

— The backup script must be run when the synchronized OpenDJ instance is `online`.

— The restore script must be run when the unsynchronized OpenDJ instance is `offline`.

— The backup and restore commands must be run as `opendj` user.

This example outlines the scenario where there are two database nodes (DB-1 and DB-2) and the OpenDJ instance is down on one of the nodes. See `opendjhost1`:

```
Server port: <port> = 1636 (default in ENM)
Host name or IP address of the first server: <hostname1> = opendjhost0 (default alias in ENM)
Host name or IP address of the second server: <hostname2> = opendjhost1 (default alias in ENM)
Password to use to bind to the server: <password> = ldapadmin (depends on the environment)

Server administration port: <portadm> = 4444 (default in ENM)

Path to OpenDJ main folder: <pathtoopendj> = /opt/opendj
Path to the target directory for the backup file: <backup_dir> = /opt/opendj/bak
Path to the target directory for the backup log file: <log_dir> = /opt/opendj/bak_log
Search base DN: <basedn> = "dc=ieatclvmlms927-1,dc=com" (depends on the environment)
```

The `<basedn>` value depends on the `COM_INF_LDAP_ROOT_SUFFIX` value, which can be found in the page 354) or by running `status` command on db node:

```
[root@ieatrcxb4363 bin]# status --offline | grep userRoot
dc=ieatlms4407,dc=com : userRoot  : DB   : Enabled
```

The `<backup_dir>` and `<log_dir>` can be any directories.

Note: The `opendj_backup.sh` script automatically creates the *<backup_dir>* and *<log_dir>* directories. If you decide to use existing directories, rather than the ones listed, ensure they can be accessed as `opendj` user.

The `<password>` is different for each installation.

All values must be used as in the following steps:

Steps

1. Verify that two OpenDJ instances are unsynchronized.

   On any server, run the following commands, and check if the total number of matching entries is the same for both DB nodes. Replace `<port>`, `<password>` , and `<basedn>` with appropriate values:

   ```
   # /opt/opendj/bin/ldapsearch -h opendjhost0 -p <port> --useSSL --trustAll -D "cn=directory manager" -w <password> -b <basedn> --countEntries "(objectclass=*)" | grep Total

   # /opt/opendj/bin/ldapsearch -h opendjhost1 -p <port> --useSSL --trustAll -D "cn=directory manager" -w <password> -b <basedn> --countEntries "(objectclass=*)" | grep Total
   ```

   Example

   ```
   [root@ieatrcxb3028 ]# /opt/opendj/bin/ldapsearch -h opendjhost0 -p 1636 --useSSL --trustAll -D "cn=directory manager" -w ldapadmin -b "dc=ieatclvmlms927-1,dc=com" --countEntries "(objectclass=*)" | grep Total
   # Total number of matching entries: 1032
   ```

```
[root@ieatrcxb3028 ]# /opt/opendj/bin/ldapsearch -h opendjhost1 -p 1636 --us →
eSSL --trustAll -D "cn=directory manager" -w ldapadmin -b "dc=ieatclvmlms927 →
-1,dc=com" --countEntries "(objectclass=*)" | grep Total
# Total number of matching entries: 1021
```

If the number of matching entries is the same on both DB nodes, the data is in `synchronized` state and there is no need to perform any further steps. If the number of entries differ on both DB nodes, as shown in the example: (1032 and 1021), continue with the procedure.

2. As user `opendj`, create the backup of the instance of OpenDJ which was active all the time (opendjhost0) - run the following script, substituting *<backup_dir>* and *<logs_dir>* with the names of folders which store the backup and backup logs:

```
# su - opendj /opt/ericsson/com.ericsson.oss.security/idenmgmt/opendj/bin/op →
endj_backup.sh <backup_dir> <log_dir>
```

Example

```
[root@ieatrcxb3028 ]# su - opendj /opt/ericsson/com.ericsson.oss.security/id →
enmgmt/opendj/bin/opendj_backup.sh /opt/opendj/bak /opt/opendj/bak_log
Script to create opendj backup
Log file: /opt/opendj/bak_log/opendj-backup-2016-05-19:12:18:58+01:00.log201 →
6-05-19:12:18:58+01:00: hostname1: INFO: decryptOpendjPasswd request is rece →
ived ..... Processing request
2016-05-19:12:18:58+01:00: hostname1: INFO: decryptOpendjPasswd completed su →
ccessfully
opendj (pid  42215) is running...
2016-05-19:12:19:01+01:00: hostname1: Waiting for results
2016-05-19:12:19:04+01:00: hostname1: INFO: backup completed successfully
```

3. Copy the backup to the server which was previously down - run the following command:

```
# scp -r <backup_dir> litp-admin@<hostname>:<pathtoopendj>
```

Example

```
[root@ieatrcxb3028 ]# scp -r /opt/opendj/bak/ litp-admin@opendjhost1:/opt/op →
endj/
```

4. As the user `opendj` restore the outdated OpenDj instance. To restore `userRoot`, `schema`, `replicationChanges`, and `backends` run the following script on the server which was previously down. Make sure OpenDJ is in `offline` state on that server:

```
# su - opendj /opt/ericsson/com.ericsson.oss.security/idenmgmt/opendj/bin/op →
endj_restore.sh <backup_dir> <log_dir>
```

Example

```
[root@ieatrcxb3211 ]# su - opendj /opt/ericsson/com.ericsson.oss.security/id →
enmgmt/opendj/bin/opendj_restore.sh /opt/opendj/bak /opt/opendj/bak_log
Script to restore opendj data
Log file: /opt/opendj/bak_log/opendj-restore-2016-09-01:08:06:30+01:00.logop →
endj is stopped
[01/09/2016:08:06:39 +0100] category=UTIL seq=0 severity=INFO msg=Restored b →
```

```
ackup file: 01-pwpolicy.ldif (size 6545)
[01/09/2016:08:06:39 +0100] category=UTIL seq=1 severity=INFO msg=Restored b →
ackup file: 03-rfc2713.ldif (size 3510)
[01/09/2016:08:06:39 +0100] category=UTIL seq=2 severity=INFO msg=Restored b →
ackup file: 99-user.ldif (size 4256)
[01/09/2016:08:06:39 +0100] category=UTIL seq=3 severity=INFO msg=Restored b →
ackup file: 03-changelog.ldif (size 5007)
[01/09/2016:08:06:39 +0100] category=UTIL seq=4 severity=INFO msg=Restored b →
ackup file: 05-solaris.ldif (size 14090)
[01/09/2016:08:06:39 +0100] category=UTIL seq=5 severity=INFO msg=Restored b →
ackup file: 05-rfc4876.ldif (size 6288)
[01/09/2016:08:06:39 +0100] category=UTIL seq=6 severity=INFO msg=Restored b →
ackup file: 03-rfc2926.ldif (size 3221)
[01/09/2016:08:06:39 +0100] category=UTIL seq=7 severity=INFO msg=Restored b →
ackup file: 03-rfc3712.ldif (size 12601)
[01/09/2016:08:06:39 +0100] category=UTIL seq=8 severity=INFO msg=Restored b →
ackup file: 00-core.ldif (size 44096)
[01/09/2016:08:06:39 +0100] category=UTIL seq=9 severity=INFO msg=Restored b →
ackup file: 02-config.ldif (size 200763)
[01/09/2016:08:06:39 +0100] category=UTIL seq=10 severity=INFO msg=Restored  →
backup file: 06-compat.ldif (size 1309)
[01/09/2016:08:06:39 +0100] category=UTIL seq=11 severity=INFO msg=Restored  →
backup file: 03-rfc3112.ldif (size 1659)
[01/09/2016:08:06:39 +0100] category=UTIL seq=12 severity=INFO msg=Restored  →
backup file: 04-rfc2307bis.ldif (size 12156)
[01/09/2016:08:06:39 +0100] category=UTIL seq=13 severity=INFO msg=Restored  →
backup file: 03-pwpolicyextension.ldif (size 1227)
[01/09/2016:08:06:39 +0100] category=UTIL seq=14 severity=INFO msg=Restored  →
backup file: 03-uddiv3.ldif (size 15807)
[01/09/2016:08:06:39 +0100] category=UTIL seq=15 severity=INFO msg=Restored  →
backup file: 03-rfc2714.ldif (size 2082)
[01/09/2016:08:06:39 +0100] category=UTIL seq=16 severity=INFO msg=Restored  →
backup file: 03-rfc2739.ldif (size 3184)
[01/09/2016:08:06:39 +0100] category=UTIL seq=17 severity=INFO msg=Restored  →
backup file: 05-samba.ldif (size 11282)
[01/09/2016:08:06:47 +0100] category=UTIL seq=0 severity=INFO msg=Restored b →
ackup file: tasks.ldif (size 6387)
[01/09/2016:08:06:56 +0100] category=UTIL seq=0 severity=INFO msg=Restored b →
ackup file: dj (size 67108864)
[01/09/2016:08:06:56 +0100] category=UTIL seq=1 severity=INFO msg=Restored b →
ackup file: dj_journal.000000000030 (size 464881)
[root@ieatrcxb3211 ]#
```

5. Bring online the OpenDJ instance which was previously down.

6. Verify that both OpenDJ instances are synchronized.

   On any server, run the following command, replacing `<hostname>` with `opendjhost0` and `opendjhost1`, and `<password>` and `<port>` with values valid for the current environment:

   ```
   # /opt/opendj/bin/ldapsearch -h <hostname> -p <port> --useSSL --trustAll -D  →
   "cn=directory manager" -w <password> -b "" --countEntries "(objectclass=*)"  →
   | grep Total
   # Total number of matching entries: 1032
   ```

   Example

   ```
   [root@ieatrcxb3211 litp-admin]# /opt/opendj/bin/ldapsearch -h opendjhost0 -p →
    1636 --useSSL --trustAll -D "cn=directory manager" -w None -b "" --countEnt →
   ries "(objectclass=*)" | grep Total
   # Total number of matching entries: 1032
   [root@ieatrcxb3211 litp-admin]# /opt/opendj/bin/ldapsearch -h opendjhost1 -p →
    1636 --useSSL --trustAll -D "cn=directory manager" -w None -b "" --countEnt →
   ries "(objectclass=*)" | grep Total
   # Total number of matching entries: 1032
   [root@ieatrcxb3211 litp-admin]#
   ```

   If both databases have the same number of matching entries, it confirms that the synchronization is complete.

Results

Both instances of OpenDJ are synchronized.

7.11 SMRS Administration Task

> This section contains the routine operation and maintenance tasks related to the administration of SMRS applications.

7.11.1 SMRS Housekeeping Configurable Parameters

Since Software Management Distribution Repository Services (SMRS) is used by multiple applications in ENM to store different kind of files, it can lead to memory issues if the file system is filled up. To avoid these kind of situations, the SMRS Housekeeping solution needs to be in place. With SMRS Housekeeping, you need not manually delete the older files. SMRS performs the cleanup of files based on the configuration parameters set by the operator. SMRS Housekeeping is available for all account types.

The configuration parameters for SMRS Housekeeping are described below:

Retention policy parameters

These parameters specify the number of node files to keep on the file system. When the number of files exceeds the specified number, older files are deleted. The retention policies used for the Housekeeping node files are stored in SMRS and are specific to each node type for which a retention policy is created.

Example: For the account Type BACKUP of ERBS node type , if the retention policy provides maximum count of files to keep is 5, SMRS Housekeeping retains the latest five files and deletes the rest of the files.

Schedule Time Parameters

SMRS housekeeping runs on a daily basis at 3 AM by default.The housekeeping service starts as per the scheduler details and the housekeeping service reads all the retention policies and deletes the node files which are eligible for deletion.

7.11.1.1 Configuration Parameters for SMRS HouseKeeping Modeled for Each Node Type in SMRS

The following table illustrates the default values for the housekeeping scheduler and retention policies:

Parameter	Type	Default Value	Description
defaultNoOfFilesToKeep	Integer	10	The maximum number of backup files that will be stored in SMRS. If the retention policy not delivered for the node type, and if the number of backup files exceeds the default count, the older backup files will be deleted as part of SMRS housekeeping.
shmNfvoSwPackagesRetentionInMinutes	Integer	60	The minimum number of minutes that NFVO-bound software package archives will be stored in the SMRS. Any older software package archives will be deleted as part of the SMRS NFVO onboarding housekeeping cycle. The SMRS NFVO onboarding housekeeping cycle is executed at the top of every hour.
SMRS_BSC_NoOf_BACKUP_FILES	Integer	2	The maximum number of BSC backup files that will be stored in SMRS. If the number of BSC backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_CSCF_NoOf_BACKUP_FILES	Integer	3	The maximum number of CSCF backup files that will be stored in SMRS. If the number of CSCF backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_DSC_NoOf_BACKUP_FILES	Integer	2	The maximum number of DSC backup files that will be stored in SMRS. If the number of DSC backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_ERBS_NoOf_BACKUP_FILES	Integer	3	The maximum number of ERBS backup files that will be stored in SMRS. If the number of ERBS backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_HLRFE_NoOf_BACKUP_FILES	Integer	2	The maximum number of HLR-FE backup files that will be stored in SMRS. If the number of HLR-FE backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_HLRFEBSP_NoOf_BACKUP_FILES	Integer	2	The maximum number of HLR-FE-BSP backup files that will be stored in SMRS. If the number of HLR-FE-BSP backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_HLRFEIS_NoOf_BACKUP_FILES	Integer	2	The maximum number of HLR-FE-IS backup files that will be stored in SMRS. If the number of HLR-FE-IS backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.

Parameter	Type	Default Value	Description
SMRS_IPSTP_NoOf_BACKUP_FILES	Integer	2	The maximum number of IP-STP backup files that will be stored in SMRS. If the number of IP-STP backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_IPSTPBSP_NoOf_BACKUP_FILES	Integer	2	The maximum number of IP-STP-BSP backup files that will be stored in SMRS. If the number of IP-STP-BSP backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_IPWorks_NoOf_BACKUP_FILES	Integer	3	The maximum number of IPworks backup files that will be stored in SMRS. If the number of IPworks backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_MGW_NoOf_BACKUP_FILES	Integer	5	The maximum number of MGW backup files that will be stored in SMRS. If the number of MGW backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_MINILINKIndoor_NoOf_BACKUP_FILES	Integer	5	The maximum number of MINILINKIndoor backup files that will be stored in SMRS. If the number of MINILINKIndoor backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_MINILINKOutdoor_NoOf_BACKUP_FILES	Integer	5	The maximum number of MINILINKOutdoor backup files that will be stored in SMRS. If the number of MINILINKOutdoor backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_MSCBCBSP_NoOf_BACKUP_FILES	Integer	2	The maximum number of MSC-BC-BSP backup files that will be stored in SMRS. If the number of MSC-BC-BSP backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_MSCBCIS_NoOf_BACKUP_FILES	Integer	2	The maximum number of MSC-BC-IS backup files that will be stored in SMRS. If the number of MSC-BC-IS backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_MSCDB_NoOf_BACKUP_FILES	Integer	2	The maximum number of MSC-DB backup files that will be stored in SMRS. If the number of MSC-DB backup files exceeds the specified count, the older backup files will be

Parameter	Type	Default Value	Description
			deleted as part of SMRS housekeeping.
SMRS_MSCDBBSP_NoOf_BACKUP_FILES	Integer	2	The maximum number of MSC-DB-BSP backup files that will be stored in SMRS. If the number of MSC-DB-BSP backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_MTAS_NoOf_BACKUP_FILES	Integer	3	The maximum number of MTAS backup files that will be stored in SMRS. If the number of MTAS backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_RadioNode_NoOf_BACKUP_FILES	Integer	3	The maximum number of RadioNode backup files that will be stored in SMRS. If the number of RadioNode backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_RBS_NoOf_BACKUP_FILES	Integer	5	The maximum number of RBS backup files that will be stored in SMRS. If the number of RBS backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_RNC_NoOf_BACKUP_FILES	Integer	5	The maximum number of RNC backup files that will be stored in SMRS. If the number of RNC backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_Router6672_NoOf_BACKUP_FILES	Integer	5	The maximum number of Router6672 backup files that will be stored in SMRS. If the number of Router6672 backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_Router6675_NoOf_BACKUP_FILES	Integer	5	The maximum number of Router6675 backup files that will be stored in SMRS. If the number of Router6675 backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_Router6x71_NoOf_BACKUP_FILES	Integer	5	The maximum number of Router6x71 backup files that will be stored in SMRS. If the number of Router6x71 backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_Router6274_NoOf_BACKUP_FILES	Integer	5	The maximum number of Router6274 backup files that will be stored in SMRS. If the number of Router6274 backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.

Parameter	Type	Default Value	Description
SMRS_Router6273_NoOf_BACKUP_FILES	Integer	5	The maximum number of Router6273 backup files that will be stored in SMRS. If the number of Router6273 backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_SAPC_NoOf_BACKUP_FILES	Integer	5	The maximum number of SAPC backup files that will be stored in SMRS. If the number of SAPC backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_SBG_NoOf_BACKUP_FILES	Integer	3	The maximum number of SBG backup files that will be stored in SMRS. If the number of SBG backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_SGSNMME_NoOf_BACKUP_FILES	Integer	2	The maximum number of SGSNMME backup files that will be stored in SMRS. If the number of SGSNMME backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_vCSCF_NoOf_BACKUP_FILES	Integer	3	The maximum number of vCSCF backup files that will be stored in SMRS. If the number of vCSCF backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_vDSC_NoOf_BACKUP_FILES	Integer	3	The maximum number of vDSC backup files that will be stored in SMRS. If the number of vDSC backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_vHLRFE_NoOf_BACKUP_FILES	Integer	2	The maximum number of vHLR-FE backup files that will be stored in SMRS. If the number of vHLR-FE backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_vIPSTP_NoOf_BACKUP_FILES	Integer	2	The maximum number of vIP-STP backup files that will be stored in SMRS. If the number of vIP-STP backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_vIPWorks_NoOf_BACKUP_FILES	Integer	3	The maximum number of vIPworks backup files that will be stored in SMRS. If the number of vIPworks backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_vMSC_NoOf_BACKUP_FILES	Integer	2	The maximum number of vMSC backup files that will be stored in SMRS. If the number

Parameter	Type	Default Value	Description
			of vMSC backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_vMSCHC_NoOf_BACKUP_FILES	Integer	2	The maximum number of vMSC-HC backup files that will be stored in SMRS. If the number of vMSC-HC backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_vMTAS_NoOf_BACKUP_FILES	Integer	3	The maximum number of vMTAS backup files that will be stored in SMRS. If the number of vMTAS backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_vSAPC_NoOf_BACKUP_FILES	Integer	3	The maximum number of vSAPC backup files that will be stored in SMRS. If the number of vSAPC backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_vSBG_NoOf_BACKUP_FILES	Integer	3	The maximum number of vSBG backup files that will be stored in SMRS. If the number of vSBG backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
SMRS_vTIF_NoOf_BACKUP_FILES	Integer	3	The maximum number of vTIF backup files that will be stored in SMRS. If the number of vTIF backup files exceeds the specified count, the older backup files will be deleted as part of SMRS housekeeping.
smrsHousekeepingStartTimeInDayOfWeek	String	*	SMRS housekeeping scheduler start time in days of the week. 0 to 7 (both 0 and 7 refer to Sunday) Sun, Mon, Tue, Wed, Thu, Fri, Sat For example: dayOfWeek=3 OR dayOfWeek=Wed
smrsHousekeepingStartTimeInHour	Integer	3	SMRS housekeeping scheduler start time in hours, 0 to 23. For example: smrsHousekeepingStartTimeInHour = 3 means start time at 3:00 AM [Max value = 23 hours] [Min value = 0 hours]
smrsHousekeepingStartTimeInMinute	Integer	0	SMRS housekeeping scheduler start time in minutes, 0 to 59 only. One or more minutes within an hour. [Max value = 59 minutes] [Min value = 0 minutes]

All the parameters configurable. The default values can be updated by following the steps in one of the subchapters in Configuring PIB Parameters on page 8, depending on the environment.

7.11.2 SMRS Disk Space Monitoring

As Software Management Distribution Repository Services (SMRS) is used by multiple applications across ENM, operators should be notified of available disk space at any given moment of time.

To ease this, alerts are set in ENM System monitoring, based on free space available. This is detailed below:

Alert Description in ENM System Monitoring (ESM)

Alert 1 if disk usage is between 85% and 90% (exclusive). This is a low priority alert.

Alert 2 if disk usage is between 90% and 95% (exclusive). This is a medium priority alert.

Alert 3 if disk usage is between 95% and 100% (exclusive). This is a high priority alert.

Note: When any of the above alert conditions are reached, an internal alarm is raised in the Fault Management (FM) application.

Customization

You can also alter the limits and set operator specified limits on disk usage for the alerts described above. This can be achieved by logging into ENM System Monitor. For more information on the required steps, refer to *View/Edit Alert Definition Templates*.

7.11.3 SFTP Port Configuration

SFTP service supports on default TCP port 22. Operator has provision to use different SFTP port in addition to default port 22.

You can choose an unused port within the range 1025-65535 if you choose not to use default port 22.

You can assign SFTP port to the attribute smrs_sftp_securePort in SED during ENM Initial install or ENM upgrade.

7.12 Install or Update CNOM or UDC Software

The Core Network Operations Manager software or UDC Dashboard application may be installed or upgraded during any planned maintenance.

CNOM and UDC Dashboard have independent application lifecycles, so newer versions can be installed in older ENM versions. ENM is not providing CNOM or

UDC Dashboard installation. They are installed in a separate step after ENM installation.

Prerequisites

— Knowledge of ENM installation and upgrade.

— Access rights to ENM sufficient to perform install/upgrade.

— Access to the CNOM software package.

— Access to the UDC Dashboard software package.

To install or upgrade CNOM software or UDC Dashboard software, see Installing Core Network Operations Manager [29] or Installing UDC Dashboard [37] respectively.

7.13 Topology Browser Administration Tasks

> This chapter contains the routine operation and maintenance tasks related to the administration of Topology Browser.

7.13.1 Edit Network Element Attributes as Administrator

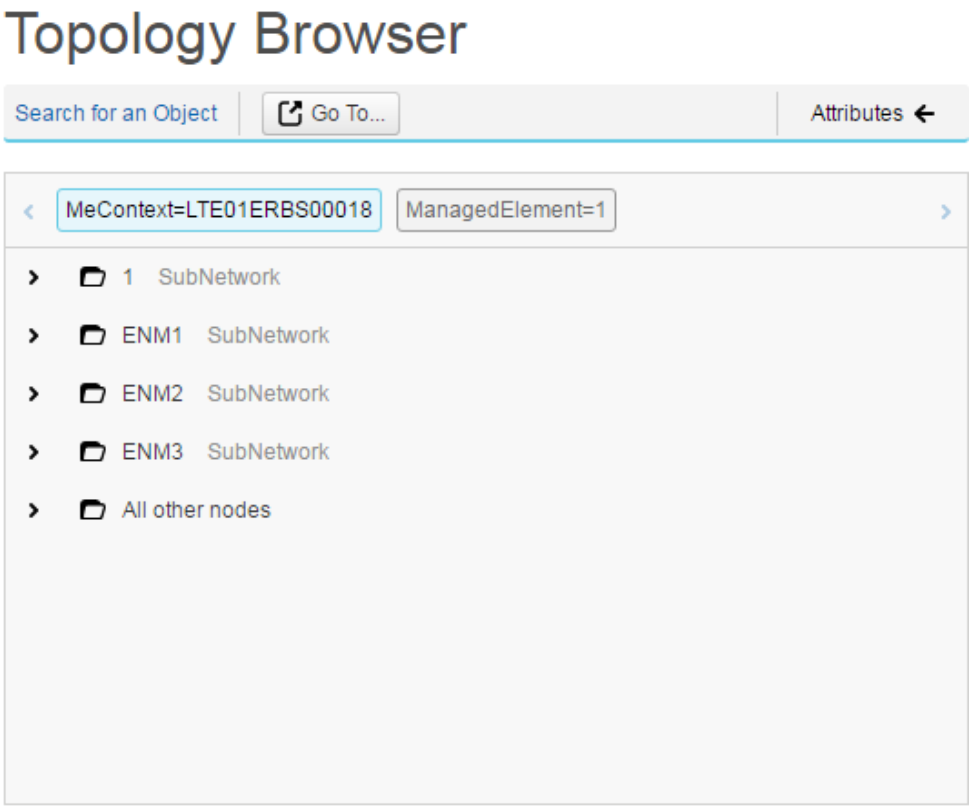
This section describes how to modify the attribute values of a Network Element within the application. It is recommended that you run this task when you want to modify node attribute information.

Prerequisites

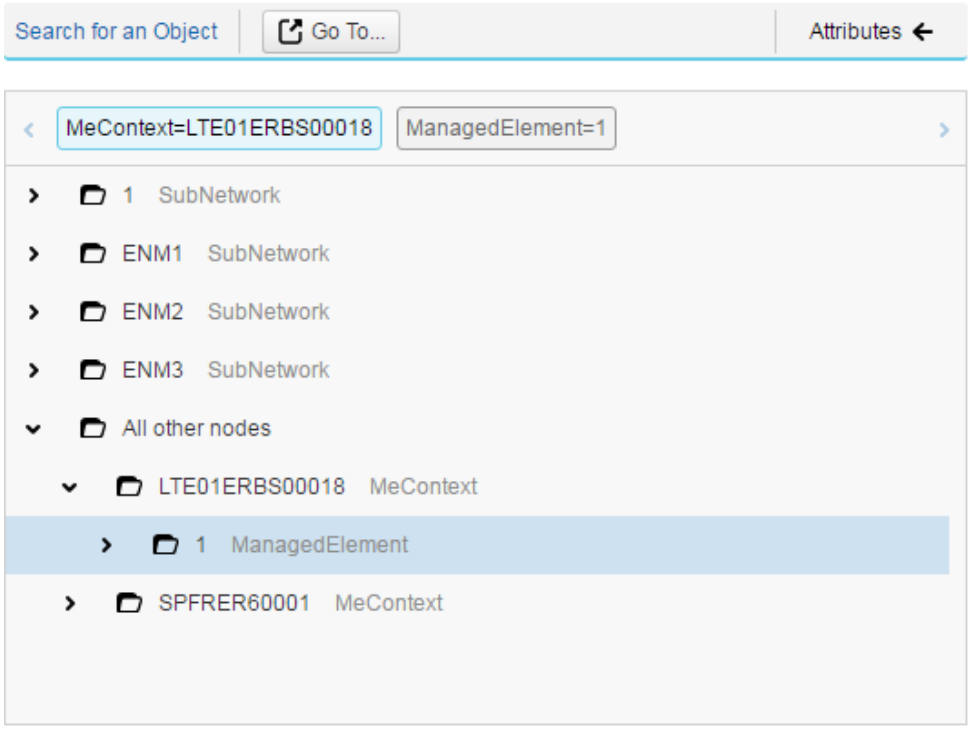
— You have Topology_Browser_Administrator rights on the system.

Steps

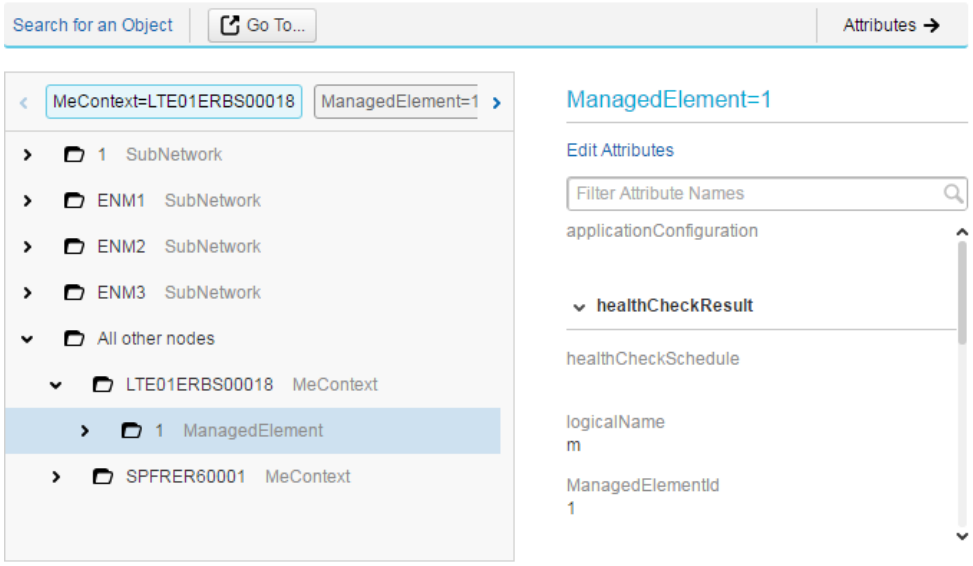
1. Launch the ENM Launcher and log on with Topology_Browser_Administrator rights.
2. Navigate to the **Topology Browser** application.



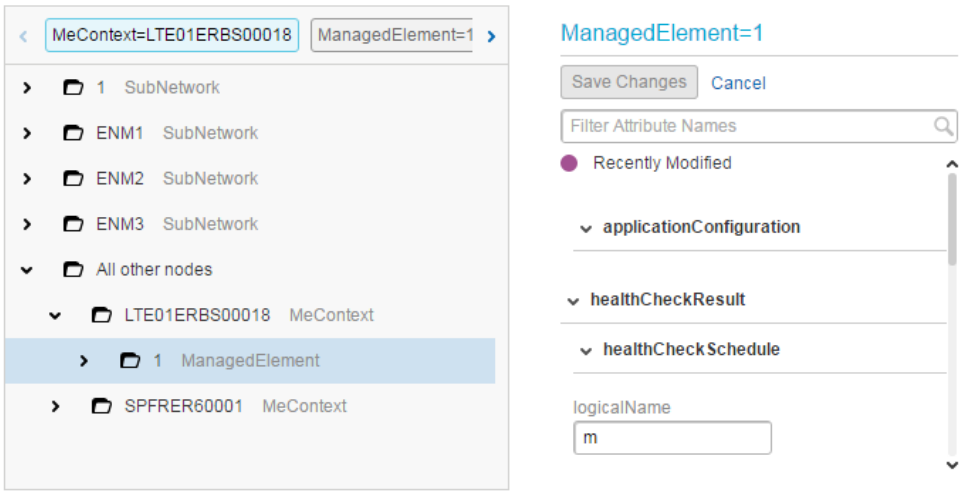
3. Select the object on the tree whose attributes you want to edit.



4. If the **Attributes** panel is not already expanded, click on the **Attributes** button in the action bar to view it.

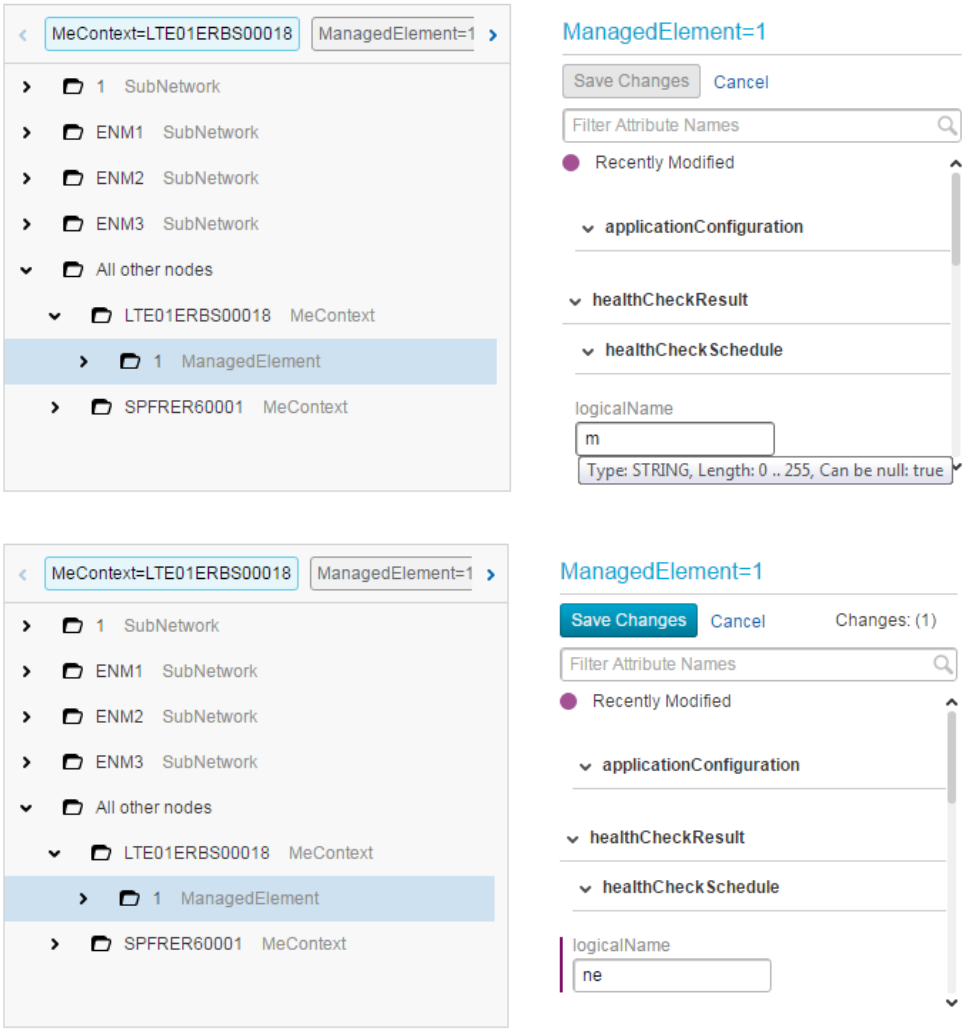


5. Click on the **Edit Attributes** link on the **Attributes** panel.



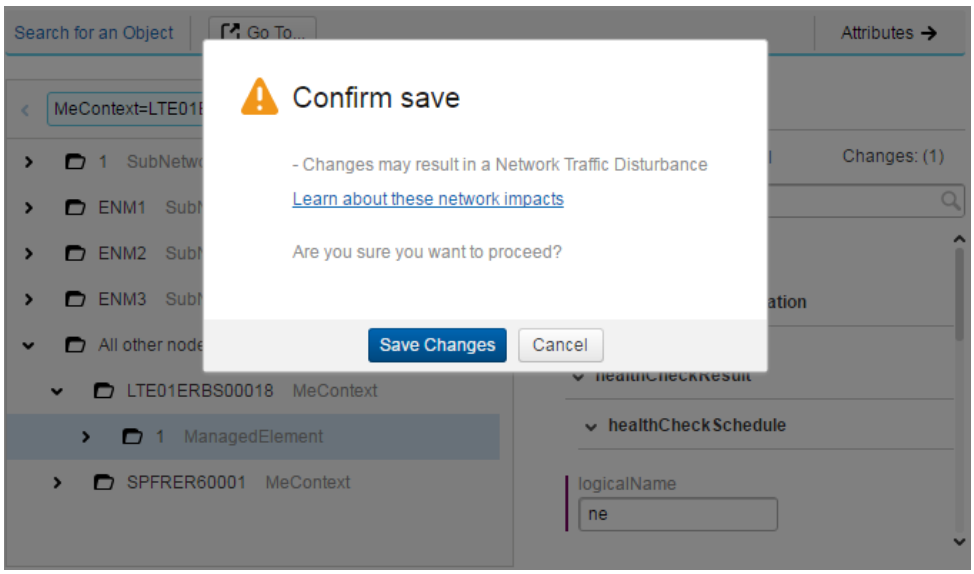
6. Select the attribute that you want to modify and apply the change.

   Note: Some attributes apply constraints. You can view these constraints by hovering your mouse over the attribute value.



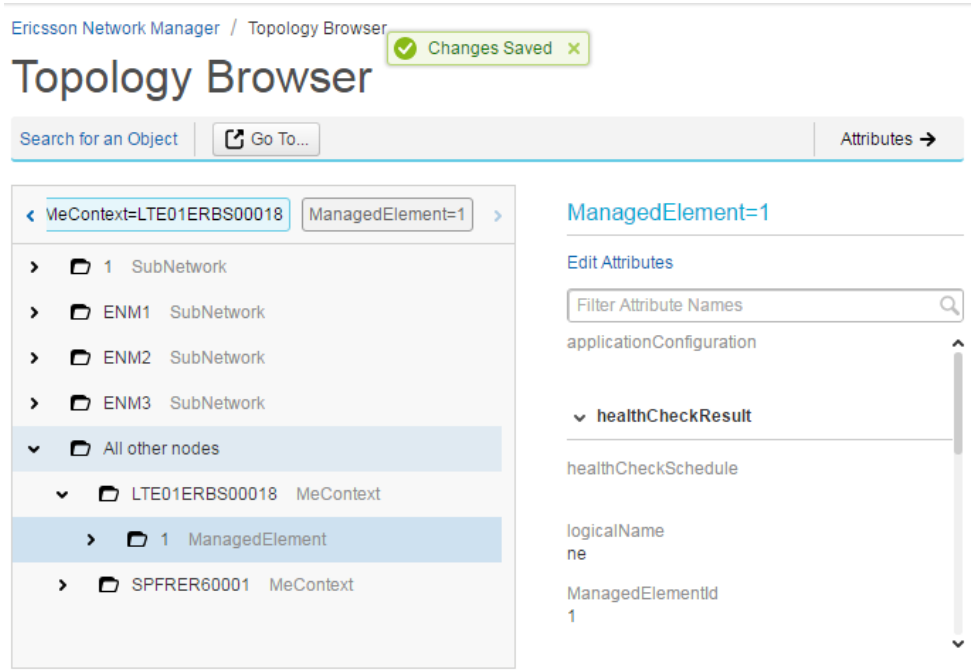
7. Click the **Save Changes** button.

   A confirmation dialog is displayed to confirm the attribute change.



8. Click the **Save Changes** button.

   Confirmation of the attribute change is displayed on screen.



7.14 ENM System Monitor Administration Tasks

> This chapter contains the routine operation and maintenance tasks related to the administration of ENM System Monitor.

7.14.1 Configure ESM for Trusted SSL Certificates

It is possible to change ESM SSL certificate configuration from default RHQ-generated keystores to ENM CA signed keystores if required to open the application using https. This procedure outlines how to configure SSL with ENM CA signed certificates.

Prerequisites

The server must have ESM installed and operational.

To configure ENM CA Signed Secure Certificates, perform the following, in the order shown.

Steps

1. Generate a Trusted JKS Format Keystore for RHQ Server on page 295
2. Configure the JKS keystore in RHQ Server on page 296
3. Generate a Trusted JKS Format Keystore for RHQ Agent on page 299
4. Configure the JKS Keystore in RHQ Agent on page 300
5. Import Root Certificates in Browser on page 302

7.14.1.1 Generate a Trusted JKS Format Keystore for RHQ Server

Generate CA signed JKS Keystore file for RHQ Server.

Prerequisites

RHQ Server must be up and running on the server where this configuration is set.

ENM Launcher User must be administrator.

Steps

1. Log on to ENM Launcher and navigate to **PKI Entity Management**.
2. In **PKI Entity Management**, create a **PKI End Entity** for RHQ Server by entering the following details.

```
Name: <Specify a entity name here>
Entity Category : SERVICE
Entity Profile : DUSGen2IPSec_SAN_CHAIN_EP
Common Name : <Specify the above given entity name here>
IP Address : <Specify Esmon vm IP here>
DNS_NAME : <Specify the hostname of Esmon vm>
Password : <Enter a password>
Count: <Enter a count number>
Validity Period: <Enter a validity period for the entity (in number)>
```

Click **Save** to save the details. An entity for RHQ Server is created.

Example

```
Name: rhqServer
Entity Category : SERVICE
Entity Profile : DUSGen2IPSec_SAN_CHAIN_EP
Common Name : rhqServer
IP Address : 192.168.0.187
DNS_NAME : enmsysmon.athtem.eei.ericsson.se
Password : RedhatServer@1
Count: 10
Validity Period: 1440
```

3. Go back to ENM Launcher page and navigate to **Command Line Interface**.
4. Execute the following command to generate JKS certificate for RHQ Server.

```
pkiadm ctm EECert -gen -nocsr -en <Specify Entity Name here> -f JKS -pass <S →
pecify any Password here>
```

Example

```
pkiadm ctm EECert -gen -nocsr -en rhqServer -f JKS -pass secu →
red
```

Note: Remember the password entered in the above command because it has to be specified in rhq server configuration file.

5. A pop-up for downloading JKS file appears, save the file locally.

7.14.1.2 Configure the JKS keystore in RHQ Server

Configure CA signed JKS keystore file in RHQ Server for SSL Communication.

JKS file has to be configured in order to establish SSL connection on RHQ Server.

Prerequisites

RHQ Server must be up and running on the server where this configuration is set.

In order to perform this task, the JKS file generated in Generate a Trusted JKS Format Keystore for RHQ Server on page 295 is required.

Steps

1. Copy the downloaded JKS file to the following path on esmon vm `/opt/rhq/rhq-server/bin` .
2. Navigate to the following path.

   ```
   cd  /opt/rhq/rhq-server/bin
   ```

3. Give permissions and ownership to the JKS certificate file.

   ```
   chmod 777 <JKS file name>
   chown rhqadmin:rhqadmin <JKS file name>
   ```

   Example

   ```
   chmod 777 rhqServer.jks
   chown rhqadmin:rhqadmin rhqServer.jks
   ```

4. Back up a copy of `rhq-server.properties` file.

   This is an optional step. (If any configuration is lost or incorrectly specified, the backed-up file can be used as a reference).

   ```
   cp rhq-server.properties rhq-server.properties.bkp
   ```

5. Open `rhq-server.properties` and modify the following configuration parameters:

   ```
       rhq.communications.connector.transport=sslservlet
       rhq.server.tomcat.security.keystore.alias= <Specify the R
   HQ Server entity name here>
       rhq.server.tomcat.security.keystore.file= <Specify the pa
   th of RHQ Server JKS file>
       rhq.server.tomcat.security.keystore.password= <Specify th
   e password given in Step 4 of Section "Generate a Trusted JKS
    Format Keystore for RHQ Server">
       rhq.communications.connector.security.keystore.file= <Spe
   cify the path of RHQ Server JKS file>
       rhq.communications.connector.security.keystore.password=
   <Specify the password given in Step 4 of Section "Generate a
   Trusted JKS Format Keystore for RHQ Server">
       rhq.communications.connector.security.keystore.key-passwo
   rd= <Specify the password given in Step 4 of Section "Generat
   e a Trusted JKS Format Keystore for RHQ Server">
       rhq.communications.connector.security.keystore.alias= <Sp
   ```

```
ecify the RHQ Server entity name here>
    rhq.communications.connector.security.client-auth-mode=ne →
ed
    rhq.server.client.security.keystore.file= <Specify the pa →
th of RHQ Server JKS file>
    rhq.server.client.security.keystore.password= <Specify th →
e password given in Step 4 of Section "Generate a Trusted JKS →
 Format Keystore for RHQ Server">
    rhq.server.client.security.keystore.key-password= <Specif →
y the password given in Step 4 of Section "Generate a Trusted →
 JKS Format Keystore for RHQ Server">
    rhq.server.client.security.keystore.alias= <Specify the R →
HQ Server entity name here>
    rhq.server.client.security.server-auth-mode-enabled=true
```

Example

```
rhq.communications.connector.transport=sslservlet
    rhq.server.tomcat.security.keystore.alias=rhqServer
    rhq.server.tomcat.security.keystore.file=/opt/rhq/rhq-ser →
ver/bin/rhqServer.jks
    rhq.server.tomcat.security.keystore.password=secured
    rhq.communications.connector.security.keystore.file=/opt/ →
rhq/rhq-server/bin/rhqServer.jks
    rhq.communications.connector.security.keystore.password=s →
ecured
    rhq.communications.connector.security.keystore.key-passwo →
rd=secured
    rhq.communications.connector.security.keystore.alias=rhqS →
erver
    rhq.communications.connector.security.client-auth-mode=ne →
ed
    rhq.server.client.security.keystore.file=/opt/rhq/rhq-ser →
ver/bin/rhqServer.jks
    rhq.server.client.security.keystore.password=secured
    rhq.server.client.security.keystore.key-password=secured
    rhq.server.client.security.keystore.alias=rhqServer
    rhq.server.client.security.server-auth-mode-enabled=true
```

6. Navigate to the following path.

```
cd /opt/rhq/rhq-server/jbossas/standalone/configuration
```

7. Backup `standalone-full.xml` to `standalone-full.xml.bkp`.

   This is an optional step (same as step 4).

8. Edit `standalone-full.xml` and make the following configuration changes.

```
<ssl key-alias="<Specify the entity name here>"  password="<Specify the JKS
Password here>" certificate-key-file="<Specify the JKS file path here>" veri
fy-client="false"
```

Example

```
<ssl key-alias="rhqServer" password="secured" certificate-key
-file="/opt/rhq/rhq-server/bin/rhqServer.jks" verify-client="
false"
```

9. Restart RHQ Server.

```
service rhq-server restart
```

10. The setup on RHQ Server is now completed. After RHQ Server is restarted, verify whether ESM GUI is accessible.

11. Executing the following command, verify whether RHQ Server is using SSL Communication.

```
/usr/bin/openssl s_client -showcerts -connect <esmon ip>:7443
```

7.14.1.3 Generate a Trusted JKS Format Keystore for RHQ Agent

Generate CA signed JKS keystore file for RHQ Agent.

Prerequisites

RHQ Agent must be up and running on the server where this configuration is set.

Note: It is up to the user to generate separate JKS files for each RHQ Agent (installed on all blades,MS and Esmon vm) or to use a single JKS for all Agents.

It is recommended to use a single JKS file across all agents.

Steps

1. Similar to RHQ Server, create an end entity for RHQ Agent by entering the following details.

```
Name : <Specify a entity name here>
Entity Category : SERVICE
Entity Profile : DUSGen2IPSec_SAN_CHAIN_EP
Common Name : <Specify the above given entity name here>
IP Address : <Leave it for default value>
DNS_NAME : <Leave it for default value>
Password : <Enter a password>
Count: <Enter a count number>
Validity Period: <Enter a validity period for the entity (in number)>
```

Example

```
Name : rhqAgent
    Entity Category : SERVICE
    Entity Profile : DUSGen2IPSec_SAN_CHAIN_EP
    Common Name : rhqAgent
    IP Address : 127.0.0.1
    DNS_NAME : localhost
    Password : RedhatAgent@1
    Count: 10
    Validity Period: 1440
```

Click **Save** to save the details. An entity for RHQ Agent is created.

2. Go back to ENM Launcher page and navigate to **Command Line Interface**.
3. Execute the following command to generate JKS certificate for RHQ Agent.

```
pkiadm ctm EECert -gen -nocsr -en <Specify Entity Name here> -f JKS -pass <S →
pecify any password here>
```

Example

```
pkiadm ctm EECert -gen -nocsr -en rhqAgent -f JKS -pass secur →
ed
```

Note: Remember the password entered in the above command because it has to be specified in rhq agent configuration file.

4. A pop-up for downloading JKS file appears, save the file locally.

7.14.1.4 Configure the JKS Keystore in RHQ Agent

Configure CA signed JKS keystore file in RHQ Agent for SSL Communication.

JKS file has to be configured in RHQ Agent so that SSL Communication can be established between RHQ Server and RHQ Agent.

Prerequisites

RHQ Agent must be up and running on the server where this configuration is set.

The JKS file generated in Generate a Trusted JKS Format Keystore for RHQ Agent on page 299 is needed to do these changes.

Note: It is up to the user to generate separate JKS files for each RHQ Agent (installed on all blades,MS and Esmon vm) or to use a single JKS for all Agents.

It is recommended to use a single JKS file across all agents.

Steps

1. Copy the downloaded JKS file to the following path where RHQ agent is configured `/opt/rhq/rhq-agent/conf`.
2. Navigate to the following path `/opt/rhq/rhq-agent/conf`
3. Give permissions and ownership to the JKS certificate file.

```
chmod 777 <JKS file name>
chown rhqadmin:rhqadmin <JKS file name>
```

Example

```
chmod 777 rhqAgent.jks
chown rhqadmin:rhqadmin rhqAgent.jks
```

4. Backup a copy of `agent-configuration.xml` file

This is an optional step. If any configuration is lost or incorrectly specified, the backed up file can be used as a reference.

```
cp agent-configuration.xml agent-configuration.xml.bkp
```

5. Open `agent-configuration.xml` and modify the following configuration parameters:

Uncommend the following block and modify the parameters of jks file accordingly.

```
    <!--
    <entry key="rhq.communications.connector.security.keystore.file"          →
  value="<Specify the path of RHQ Agent JKS file>" />
    <entry key="rhq.communications.connector.security.keystore.password"      →
  value="<Specify the password given in Step 3 of Section "Generate a Truste →
d JKS Format Keystore for RHQ Agent">" />
    <entry key="rhq.communications.connector.security.keystore.key-password" →
  value="<Specify the password given in Step 3 of Section "Generate a Truste →
d JKS Format Keystore for RHQ Agent">" />
    <entry key="rhq.communications.connector.security.keystore.alias"         →
  value="<Specify the RHQ Agent entity name here>" />
    <entry key="rhq.communications.connector.security.client-auth-mode"       →
  value="need" />
    <entry key="rhq.agent.client.security.keystore.file"            value="< →
Specify the path of RHQ Agent JKS file>" />
    <entry key="rhq.agent.client.security.keystore.password"        value="< →
Specify the password given in Step 3 of Section "Generate a Trusted JKS Form →
at Keystore for RHQ Agent">" />
    <entry key="rhq.agent.client.security.keystore.key-password"    value="< →
Specify the password given in Step 3 of Section "Generate a Trusted JKS Form →
at Keystore for RHQ Agent">" />
    <entry key="rhq.agent.client.security.keystore.alias"           value="< →
Specify the RHQ Agent entity name here>" />
```

```
    <entry key="rhq.agent.client.security.server-auth-mode-enabled" value="t
rue" />
    -->
```

Example

```
 <entry key="rhq.communications.connector.security.keystore.f
ile" value="/opt/rhq/rhq-agent/conf/rhqAgent.jks"/>
    <entry key="rhq.communications.connector.security.keystor
e.password" value="secured"/>
    <entry key="rhq.communications.connector.security.keystor
e.key-password" value="secured"/>
    <entry key="rhq.communications.connector.security.keystor
e.alias" value="rhqAgent"/>
    <entry key="rhq.communications.connector.security.client-
auth-mode" value="need"/>
    <entry key="rhq.agent.client.security.keystore.file" valu
e="/opt/rhq/rhq-agent/conf/rhqAgent.jks"/>
    <entry key="rhq.agent.client.security.keystore.password"
value="secured"/>
    <entry key="rhq.agent.client.security.keystore.key-passwo
rd" value="secured"/>
    <entry key="rhq.agent.client.security.keystore.alias" val
ue="rhqAgent"/>
    <entry key="rhq.agent.client.security.server-auth-mode-en
abled" value="true"/>
```

6. Stop RHQ Agent.

```
service rhq-agent stop
```

7. Perform Cleanconfig on RHQ Agent.

```
 service rhq-agent cleanconfig
```

8. The setup on RHQ Agent is now completed. In order to test whether Agent is communicating with Server, login to ESM GUI, check whether the agent is available and metrics for that agent are collected.

7.14.1.5 Import Root Certificates in Browser

Import Root CA Certificates in browser for Secured ESM Communication.

Prerequisites

ESM must be configured with SSL Communication.

The ESM user should be esmadmin where as the ENM Launcher user should be administrator

Steps

1. Open ENM Launcher and navigate to **Command Line Interface**. Execute the following commands:

   ```
   pkiadm ctm CACert -expcert -en NE_IPsec_CA -f PEM
   pkiadm ctm CACert -expcert -en ENM_PKI_Root_CA -f PEM
   ```

2. Pop-ups to download the certificates (NE_IPsec_CA and ENM_PKI_Root_CA) appear, save them locally.
3. Re-name the saved files from extension `pem` to `crt`.

   Example

   — `NM_PKI_Root_CA.pem` to `ENM_PKI_Root_CA.crt`

   — `NE_IPsec_CA.pem` to `NE_IPsec_CA.crt`
4. Open the browser, go to settings > **Advanced Settings** > **Certificates** section.
5. Import `NE_IPsec_CA.crt` to "Intermediate Certification Authorities" and `ENM_PKI_Root_CA.crt` to "Trusted Root Certifications" .
6. Open ESM GUI from the same browser. In the URL https must be shown as Secure without any error mark or a red crossed mark on https.
7. SSL on ESM is now completely configured.
8. Verify the below test cases:

   a. ESM GUI is opening properly or not with https.

   b. All RHQ Agents must be up and running and they must be in available state in GUI.

   c. Metrics are properly collected for the agents.

7.14.2 Renewal of Trusted SSL Certificates for ESM After Upgrade

This section describes the procedure to renew the following trusted SSL certificates after upgrade:

— Trusted JKS Format Keystore for RHQ Server

— Trusted JKS Format Keystore for RHQ Agent

7.14.2.1 Renewal of a Trusted JKS Format Keystore for RHQ Server

After a successful upgrade, to renew a trusted JKS format keystore for RHQ Server, follow the instructions specified in the Configure the JKS keystore in RHQ Server chapter.

7.14.2.2 Renewal of a Trusted JKS Format Keystore for RHQ Agent

After a successful upgrade, to renew a trusted JKS format keystore for RHQ Agent, follow the instructions specified in the Configure the JKS Keystore in RHQ Agent chapter.

7.14.3 Renewal of Expired Trusted SSL Certificates for ESM

This section describes the procedure to renew the validity of the following trusted SSL certificates for ESM:

— Trusted JKS Format Keystore for RHQ Server

— Trusted JKS Format Keystore for RHQ Agent

7.14.3.1 Renewal of an Expired Trusted JKS Format Keystore for RHQ Server

> Do the following to renew the validity of a trusted JKS format keystore for RHQ Server.

1. Log on to the ENM Launcher and navigate to PKI Entity Management.
2. Search for the existing RHQ Server JKS keystore and select it.
3. Click **Delete**.
4. Follow the instructions specified in the Generate a Trusted JKS Format Keystore for RHQ Server chapter.
5. Log on to the Esmon VM and navigate to the following:

   ```
   [root@ms-esmon configuration]#cd /opt/rhq/rhq-server/bin
   [root@ms-esmon configuration]#
   ```

6. Remove the existing rhq-server JKS file.

   Example

   ```
   rm -rf XXXXXX.jks
   ```

7. Follow the instructions specified in the Configure the JKS keystore in RHQ Server chapter and configure the JKS Format Keystore for RHQ Server.

7.14.3.2 Renewal of an Expired Trusted JKS Format Keystore for RHQ Agent

> Do the following to renew the validity of a trusted JKS format keystore for RHQ Agent.

1. Log on to the ENM Launcher and navigate to PKI Entity Management.
2. Search for the existing JKS keystore for RHQ Agent and select it.
3. Click **Delete**.
4. Follow the instructions specified in the Generate a Trusted JKS Format Keystore for RHQ Agent chapter.
5. Log on to the path where the RHQ Agent is configured and navigate to following path:

   ```
   [root@ieatrcxb5575 /]# cd /opt/rhq/rhq-agent/conf/
   [root@ieatrcxb5575 conf]#
   ```

6. Remove the existing rhq-agent JKS file.

   Example

   ```
   rm -rf XXXXXX.jks
   ```

7. Follow the instructions specified in the Configure the JKS Keystore in RHQ Agent chapter and configure the JKS Format Keystore for RHQ Agent.

7.14.4 Configure System Monitor Email Address

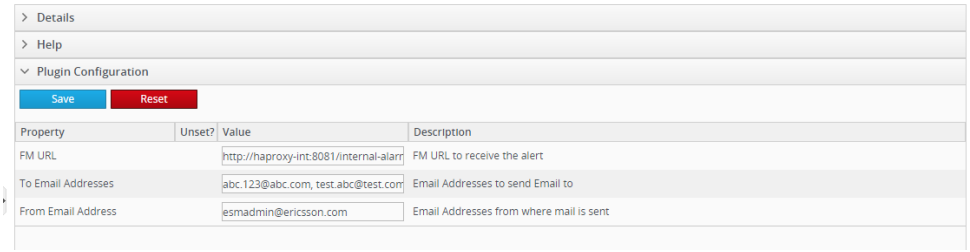
ESM provides alternate notification for alerts when FM is unreachable by sending an email notification to pre-configured email addresses.

Prerequisites

The user is logged on to ESM as esmadmin.

Steps

1. Log on to ESM.
2. Click **Administration**.
3. Click **Server Plugins** under **Configuration** tab.
4. Click **Alert:FMAlert Plugin**.
5. Click **Plugin Configuration**.



6. Specify valid email addresses in the **To Email Addresses** field separated by comma.

   Note: Spaces are not allowed between two email addresses.

7. Specify valid email address in the **From Email Address** field.

   Note: Only one valid email address is acceptable.

8. Click **Save**.

   a. As the alarms are not sent to FM, the email receiver should contact Ericsson personnel to restore the system.

   b. For the email notification on clear alarm, the email receiver has to clear the original alarm from FM. Refer to online help in FM GUI to clear alarm (**Help** > **Tutorials** > **Alarm Operations** > **Clear Alarm**)

Results

Email addresses for alerts when FM is unreachable have been configured.

7.14.5 Creating a New User

ESM user can create new user and roles

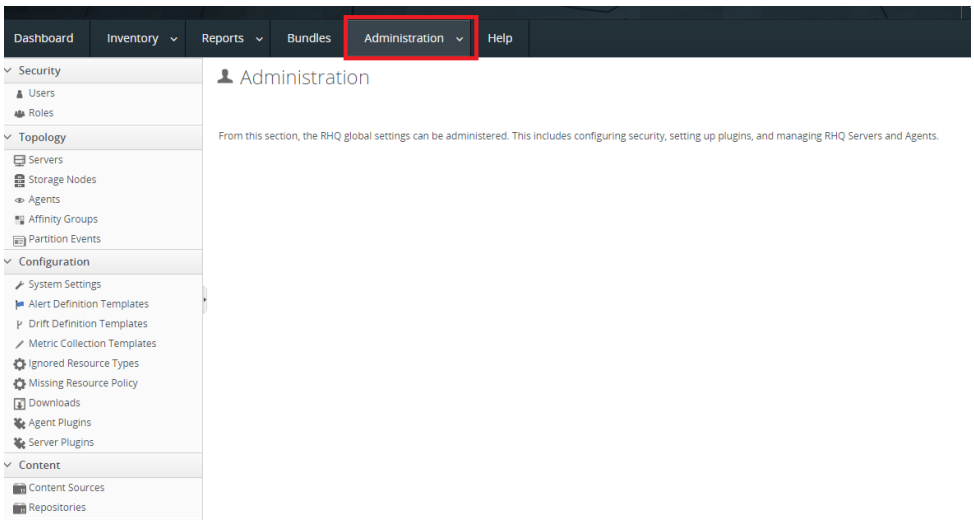
A new user ID is created with associated roles.

Prerequisites

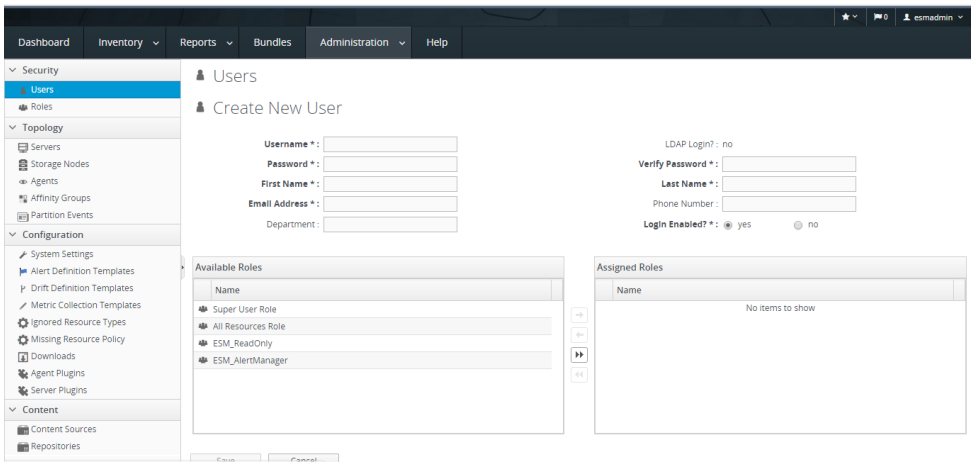
User is logged on to ESM as esmadmin.

Steps

1. Click **Administration**.



2. Click **Users** under **Security**.
3. Click **New**.
4. Enter the **Username**, **Password**, **Verify Password**, **First Name**, **Last Name**, and **Email Address**.
5. Select the role from **Available Roles**.



6. Click **Save**.

   Note: A globally uncaught exception is displayed. However, the user is created.

7.14.6 Deploy Plugins

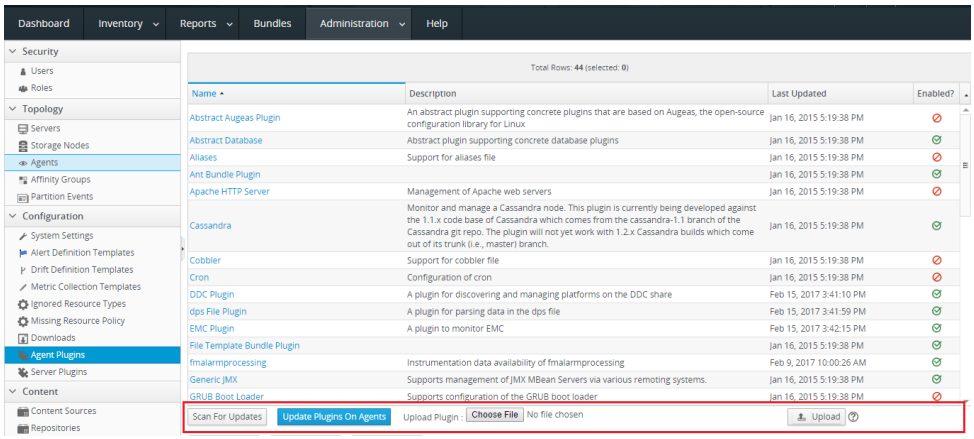
Deploy plugins allows user to install new agent/server plugins.

Prerequisites

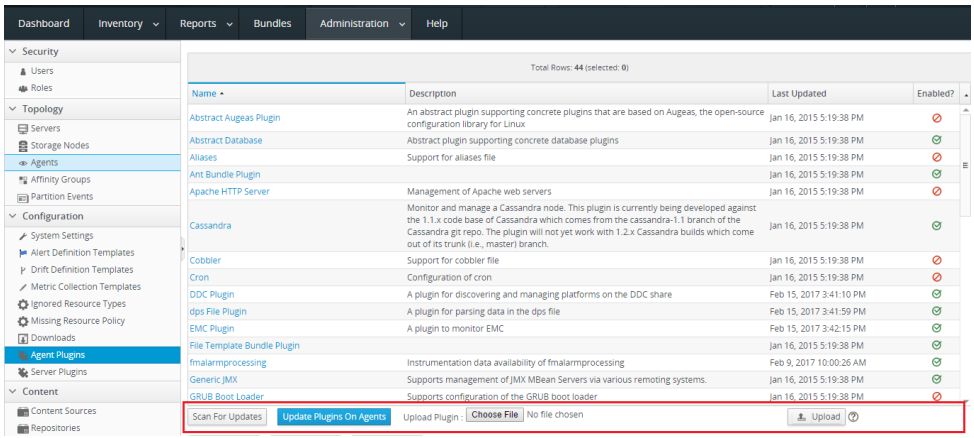
User is logged on to ESM as esmadmin.

Steps

1. Click **Administration**.



2. Click **Agent Plugins** or **Server Plugins** under the **Configuration**.
3. Click **Choose File** and add the respective plugin.



4. Click **Upload**.

7.14.7 Disable ESM Customized Plugins on all Blades

ENM System Monitor provides an interface to run the customized plugins only on esmon VM and preventing them from running on all other blades.

The plugin names included in the configuration file `/ericsson/custom/esm/excluded_plugins_on_blades.conf` are disabled on all blades except on esmon.

Prerequisites

The user is logged on to Management server as a root user.

Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.
2. Update the configuration file `excluded_plugins_on_blades.conf` with the plugin names to be disabled on all blades (with the exception of esmon).

   Add each plug-in name as a new line as shown

   ```
   # vi /ericsson/custom/esm/excluded_plugins_on_blades.conf
   ```

3. Restart the RHQ agent on all other blades so that the `prefs.xml` file is updated.

   ```
   # mco service rhq-agent restart
   ```

   Note: This feature is not applicable for cloud.

7.14.8 Exclude Resources from Raising FM Alarms

ENM System Monitor provides an interface to exclude resources, for example, file systems, CPU, from raising alarms on FM Alarm Monitor

Prerequisites

The user must be logged in to the esmon VM as root user.

Steps

1. Log on to the ENM MS as the `litp-admin` user and switch to the `root` user.

2. Update the configuration file `exclude_resources_for_fm_alarms.txt` with resource names to disable them from raising alarms:

```
# vi /ericsson/custom/esm/exclude_resources_for_fm_alarms.txt
```

Add each resource name as a new line:

```
/dev/shm
/ericsson/custom
```

7.14.9 Enable/Disable Plugins

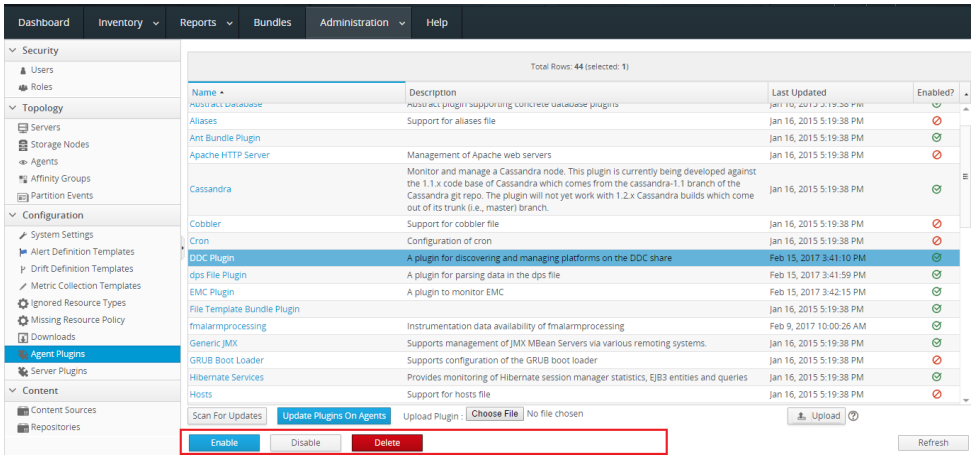
Enable/disable plugins allows user to Enable/Disable the existing plugins.

Prerequisites

User is logged on to ESM as esmadmin.

Steps

1. Click **Administration**.
2. Click **Agent/Server Plugins** under the **Configuration**.
3. Select the plugin that needs to be enabled/disabled.
4. Click **Enable** or **Disable**.



7.14.10 Enable Monitoring for EMC Clariion/VNX Storage

The EMC Clariion storage plug-in provides monitoring of the EMC Clariion and VNX Storage (5200 / 5400 / 5500) on the ESM platform.

Prerequisites

— EMC command line tool "naviseccli" has been installed and accessible at the following location on ESM VM - `/opt/Navisphere/bin/naviseccli`.

Steps

1. Configure naviseccli.

    a. Log on to the Management Server using ssh.

    b. Run the following command on MS to verify the EMC details.

    ```
    # /usr/bin/litp show -p /infrastructure/storage/storage_providers/s
    an1
    ```

    c. Run the following commands on esmon.

    ```
    # su -s /bin/sh rhqadmin -c "/opt/Navisphere/bin/naviseccli -h <spa
    _ip> -user <emc_username> -password <emc_password> -Scope 0 -AddUse
    rSecurity -secfilepath /var/ericsson/esm-data/emc/"

    # su -s /bin/sh rhqadmin -c "/opt/Navisphere/bin/naviseccli -h <spb
    _ip> -user <emc_username> -password <emc_password> -Scope 0 -AddUse
    rSecurity -secfilepath /var/ericsson/esm-data/emc/"
    ```

    d. Check if the configuration is working by running the following command.

    ```
    #  su -s /bin/sh rhqadmin -c "/opt/Navisphere/bin/naviseccli  -h <i
    p> -secfilepath /var/ericsson/esm-data/emc/ getagent -model -serial
    "
    ```

2. Import EMC into ESM.

    a. Log on to ESM as esmadmin.

    b. Click **Inventory**

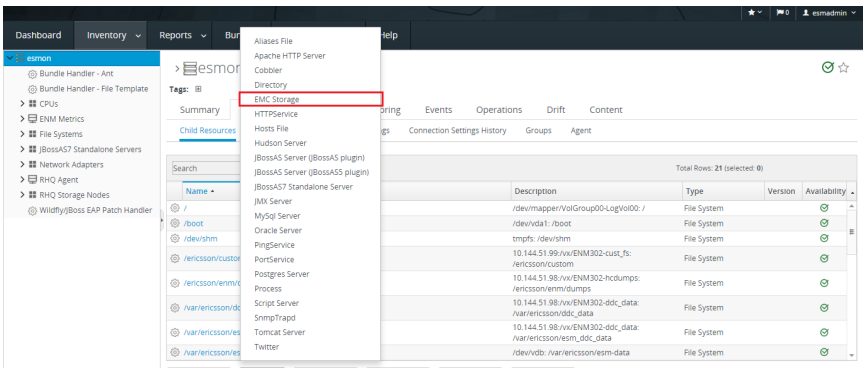
    c. Click **Platforms**.

    d. Select **esmon**

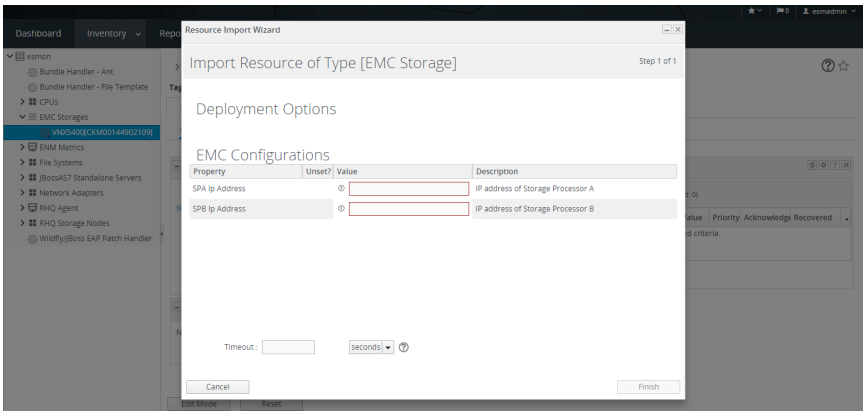
    e. Click **Inventory** subtab in esmon platform

    f. Click **import**.

    g. Select **EMC Storage**

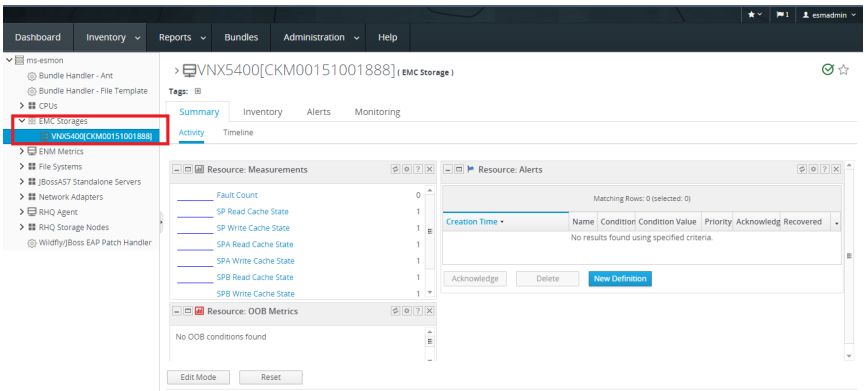


h. Enter the **IP Address for SPA** and **IP Address for SPB**. Click **Finish**.



i. EMC Storage resource is imported and metrics are displayed.

Note: This feature is not applicable for cloud.



7.14.11 Import/Export Alert Definition Templates

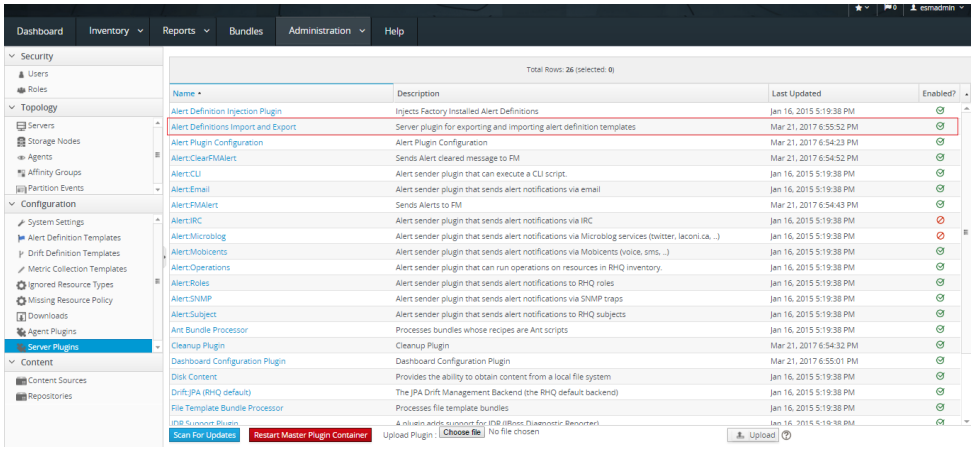
It is possible to Import/Export Alert Definition Templates. Import allows user to import the Alert Definition Templates to ESM GUI and Export allows user to export the existing Alert Definition Templates to user defined xml file.

Prerequisites

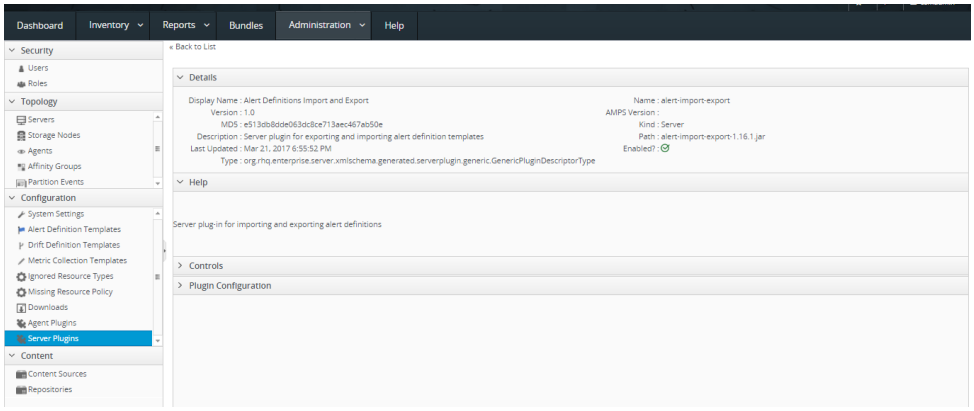
The user is logged on to ESM as esmadmin.

Steps

1. Log on to ESM.
2. Click **Administration**.
3. Click **Server Plugins** under **Configuration**.



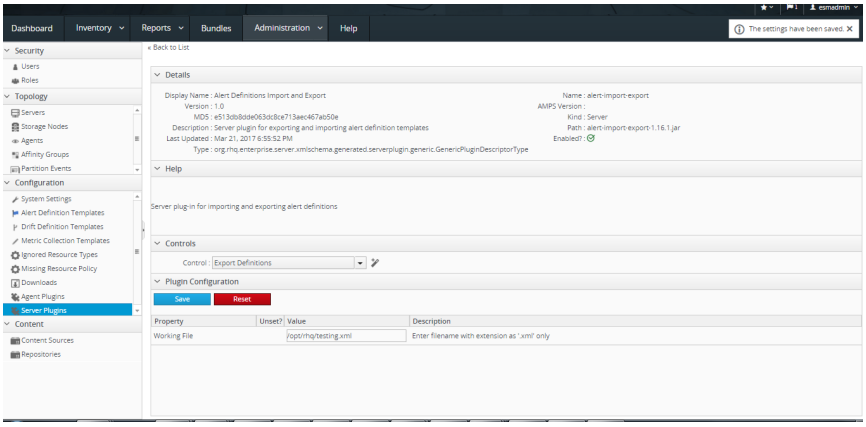
4. Click **Alert Definitions Import and Export**.



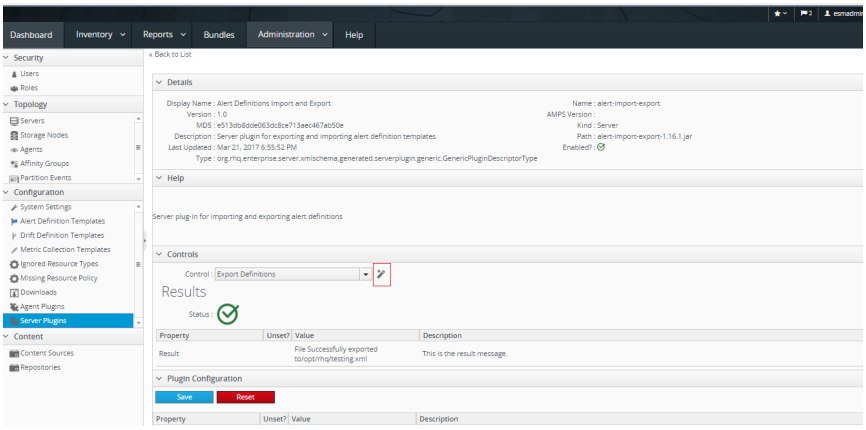
5. Export
    a. Click **Controls** and select **Export Definitions**
    b. Click **Plugin Configuration** and enter the location to where the templates are to exported in the Working File field.

        Note: Directories specified in **Working File** field must already exist, the file must be of XML format. It is necessary to have write permissions to the working file.

c. Click **Save**.



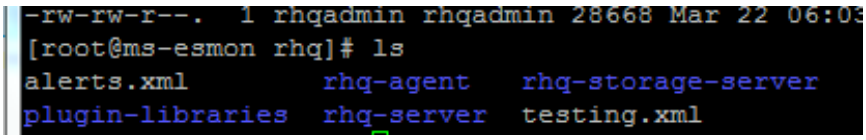
d. Click **Execute** icon



e. Connect to Server and verify that the exported file exists in the specified directory.

f. Log on to esmon.

g. Go to the path specified in working file value. The Alert Definition Templates is available in user defined xml.



6. Import

a. Click **Controls** and select **Import Definitions**.

b. Select **Yes** or **No** to Override Templates.

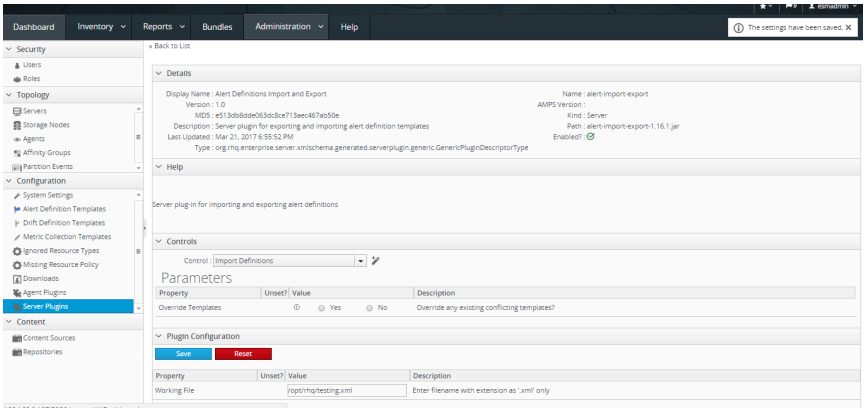
Note: If **Override Templates** is set to **Yes**, then the existing templates will be overridden with the new templates.

If **Override Templates** is set to **No**, then the existing templates will remain same and only new templates will be added.

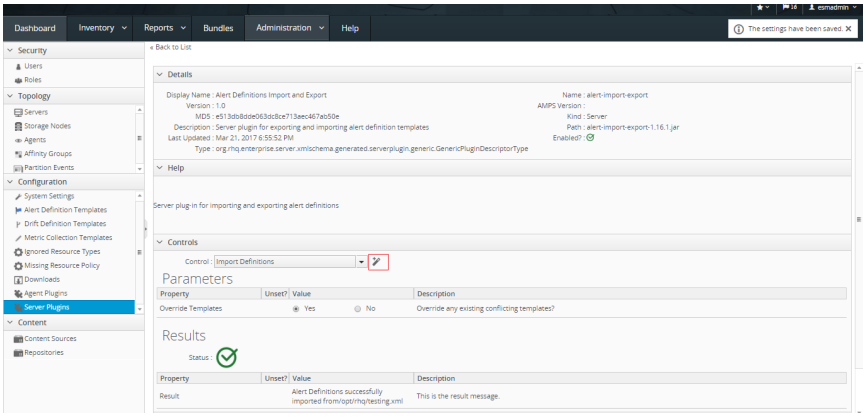
c. Copy the exported template file to the location from where the templates are to be imported.

d. Click **Plugin Configuration** and enter the location from where the templates are to imported in the **Working File** field.

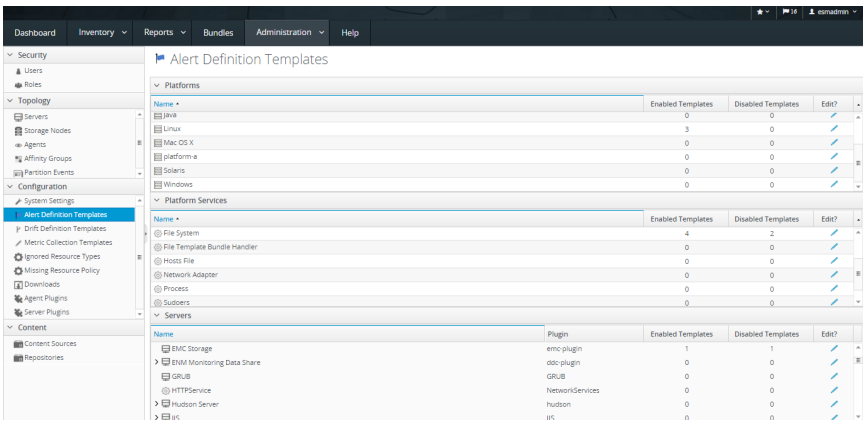
e. Click **Save**.



f. Click **Execute** icon.



g. Click **Administration** > **Alert Definition Templates** and verify the Alert Definition templates that are imported.



7.14.12 Uninventory of Resource from ESM GUI

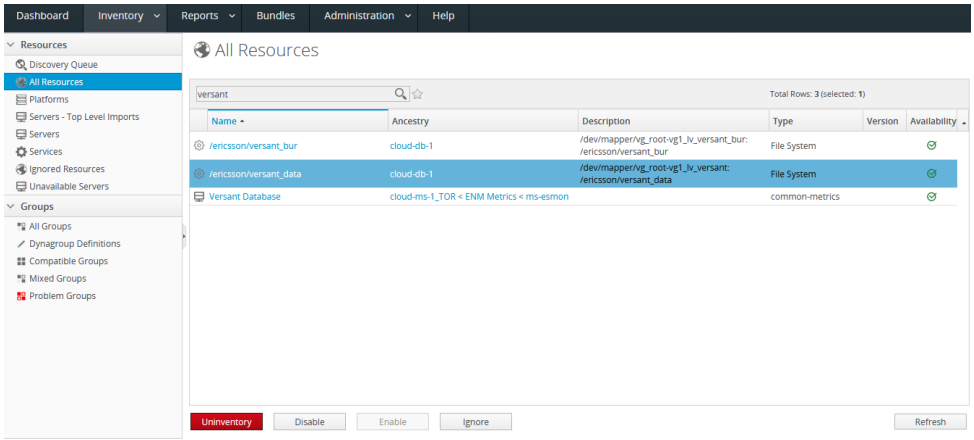
Uninventory operation allows ESM user to stop monitoring the resource.

Prerequisites

User is logged on to ESM as esmadmin.

Steps

1. Click **Inventory** > **All Resources**
2. Search and select the resource from the list displayed and click **Uninventory**.



After This Task

Note: ESM does not differentiate between temporary file system and permanent file system. When a file system is unmounted ESM still continues to monitor the FS. In order to stop ESM from monitoring that FS, **Uninventory** the resource from ESM GUI.

7.14.13 View/Edit Alert Definition Templates

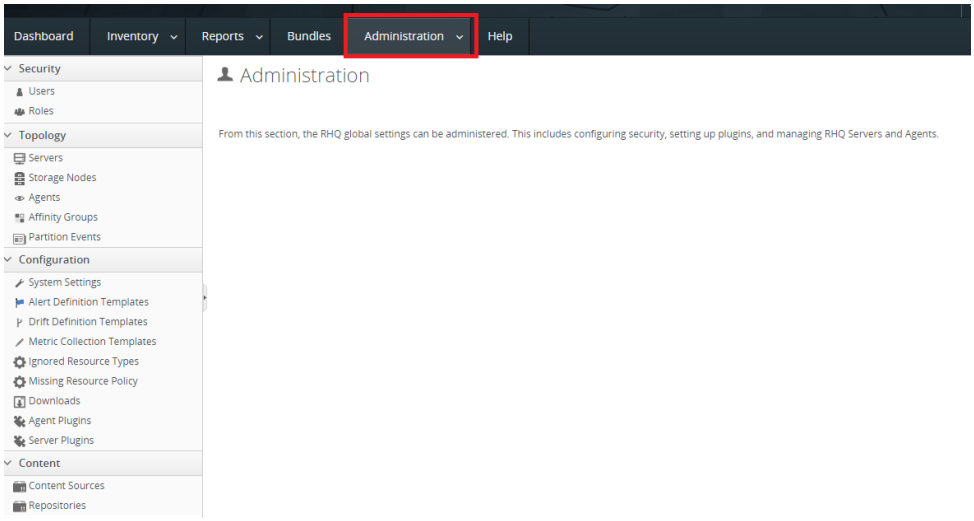
Alert Definition Templates allows user to view/edit alert definitions on all resources of the same resource type.

Prerequisites

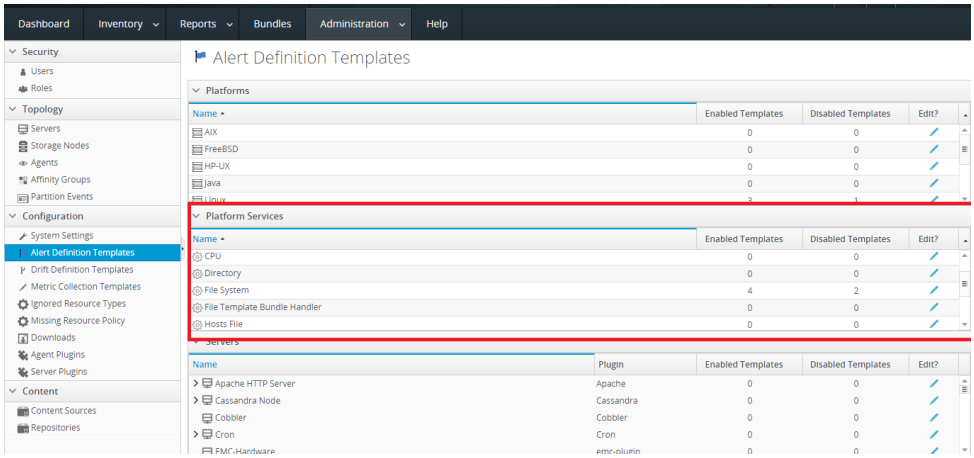
User is logged on to ESM as esmadmin.

Steps

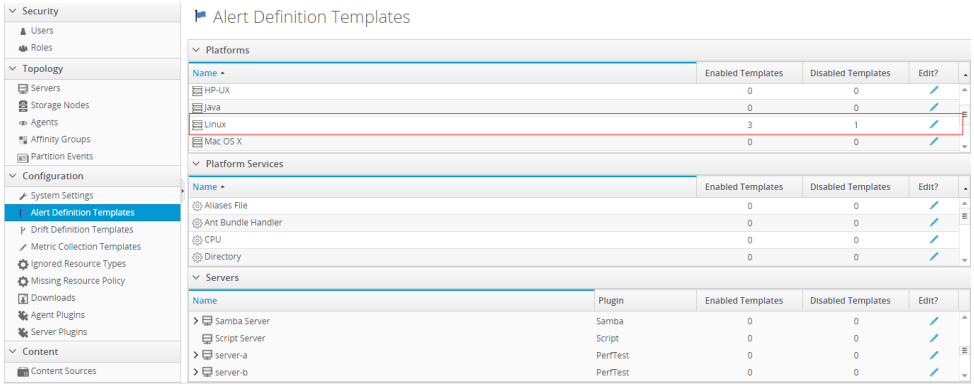
1. Click **Administration**.



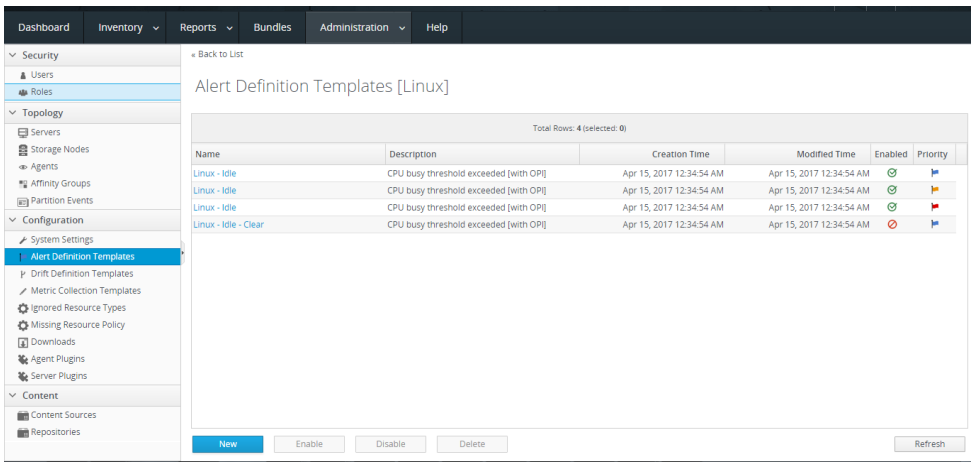
2. Go to **Alert Definition Templates** under **Configuration**.
3. Alert templates for **File System** are available under **Platform Services**.



4. Alert templates for **CPU** are available under **Platform** as **Linux**.



5. Click **Edit** for either File System or CPU to view their respective default alert definition templates and modify.



Note: Any changes to Alert Definition Templates will overwrite the existing thresholds.

After This Task

Note: Any changes to Alert Definition Templates will overwrite the existing thresholds.

7.15 Network Explorer Administration Tasks

> This chapter describes the routine operation and maintenance tasks related to the administration of Network Explorer.

7.15.1 Configure Parameters for Collections in Network Explorer

Currently Network Explorer supports configuring aspects of collections.

7.15.1.1 Change Total Number of Managed Object Instances

The root user can change the total number of Managed Object instances which can be stored in a collection by modifying the parameter `maxCollectionSizeLimit` using the Platform Integration Bridge (PIB) script.

Prerequisites

Access to the Peer Servers

Note: Service name is netex.

Steps

1. Modify the parameter `maxCollectionSizeLimit` using the Platform Integration Bridge (PIB) script.

   For details on how to view and modify PIB parameters, refer to the Configuring PIB Parameters on page 8.

2. Verify the parameter has changed using the read command.

Table 28 PIB Parameter Table

name	service_identifier	Description	Default Value
`maxCollectionSizeLimit`	`topologyCollectionsService`	Parameter to configure no. of objects which can be stored in a collection	`25,000`

7.15.2 Delete Public Collections and Saved Searches as Administrator

— The public Collections and Saved Searches of any user can be deleted by the Administrator if are no longer relevant or the user who owns them no longer exists.

— When you are logged in as Administrator, you can delete any public Collection or Saved Search. The example below shows how to delete a public Collection. The steps are the same for deleting a public Saved Search.

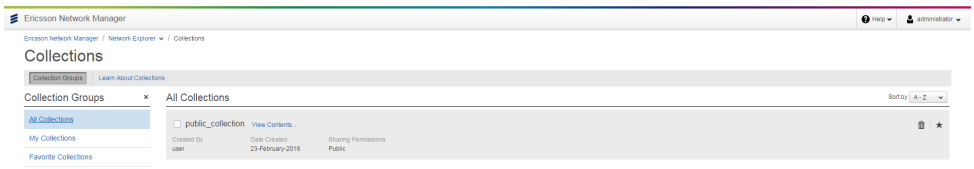
Prerequisites

— A user with Administrator role exists on the system.

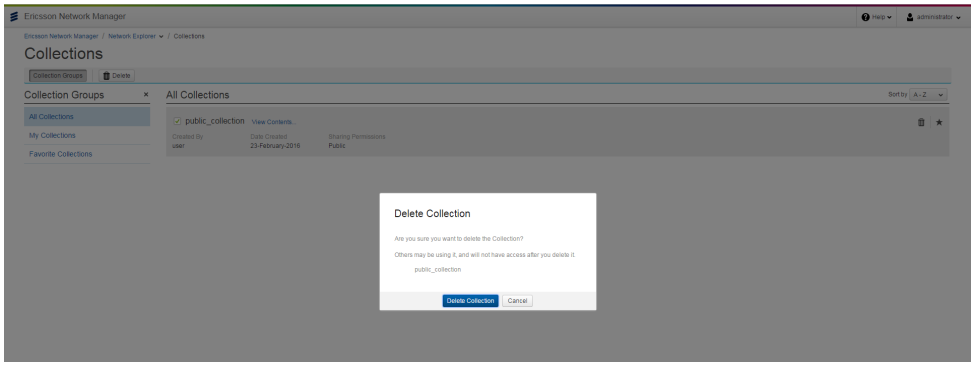
Steps

1. Log in as Administrator.

2. Navigate to **Network Explorer**, then navigate to the **Collections** page and click **View All Collections** in the sidebar. Then click **All Collections** and select the desired public Collection.



3. Click the **Delete** button in the action bar.



4. Click the **Delete Collection** button in the delete pop-up.

7.15.3 Change Default customTopologyName Value

Network Explorer supports configuring the following aspects of Collections:

— On startup, a TransportTopology is created automatically.

— The name used to create TransportTopology is determined by the parameter `customTopologyName`.

— The default value of customTopologyName is **TransportTopology**.

— The root user can change these default values using the Platform Integration Bridge (PIB) script.

Table 29 PIB Parameter Table

name	service_identifier	Description	Default Value
customTopologyName	topologyCollectionsService	Parameter to configure name of automatically generated TransportTopology	TransportToplogy

7.16 License Control Monitor Administration Tasks

This guide describes how to install and maintain ENM licenses using the License Control Monitor (LCM) service. The command syntax uses the following formatting:

— Parameters in ( ) are required

— Parameters in [ ] are optional

— Parameters in < > are expressions or variables to be replaced with a real value

7.16.1 Open ENM CLI Console

LCM commands can only be executed on the ENM CLI console. Perform the following steps to open the ENM CLI console:

Steps

1. Log on to ENM as ADMINISTRATOR or as Lcm_Administrator.
2. Select the **Command Line Interface** menu option.

7.16.2 License Enforcement

The goal of license enforcement is to block the ENM user from adding the nodes with the particular Network Element (NE) type in to the system when there is a license enforcement requirement for that particular NE type.

LTE eNodeB License Enforcement (#5MHZ Sector Carriers Price Parameter)

License permission is internally checked when an ENM user attempts to run the following command to add a node in to ENM:

```
cmedit create NetworkElement=LTE06ERBS00001 networkElementId="LTE06ERBS00001",ne →
Type="ERBS",platformType="CPP",ossModelIdentity="2827-283-011",ossPrefix="MeCont →
ext=LTE06ERBS00001" -ns=OSS_NE_DEF -v=2.0.0
```

If there is no valid license installed or the usage exceeds the capacity allowed, the following error message is displayed:

```
cmedit create NetworkElement=LTE06ERBS00001 networkElementId="LTE06ERBS00001",ne →
Type="ERBS",platformType="CPP",ossModelIdentity="2827-283-011",ossPrefix="MeCont →
ext=LTE06ERBS00001" -ns=OSS_NE_DEF -v=2.0.0
Error 9999 : Internal Error Node ID : svc-2-mscm Exception occurred: Cannot add  →
node due to invalid/inadequate license.
Suggested Solution : This is an unhandled system error, please check the error l →
og for more details.
```

The network usage for each corresponding price parameter is also collected hourly in the license control and monitoring service. If the network usage is lower than the valid license limit, adding nodes is allowed. If the network usage is higher than the valid license limit without available grace period, the adding of nodes is blocked. If there is an available grace period, the adding of nodes is allowed for the grace period with a default 14-day duration. After the grace period ends, the adding of nodes is blocked if the usage remains above the limit.

This license enforcement can be cleared by following the enforcement clearing policy, meaning adding eNodeB is allowed when installing a new license with an increased capacity limit of >= 5% and the usage is below new limit.

The enforcement scheme also works for the following:

— Capacity License: LTE #5 MHz Sector Carrier Price Parameter enforcement

— Capacity License: SGSN-MME #KSAU Price Parameter enforcement

— Capacity License: MGW #SCC Price Parameter enforcement

— Capacity License: R6000 #NodesPrice Parameter enforcement

— Capacity License: Fronthaul 6080 #Nodes Price Parameter enforcement

— Capacity License: Fronthaul 6020 #Nodes Price Parameter enforcement

— Capacity License: MINI-LINK #Nodes Price Parameter enforcement

— Capacity License: Cell Carrier #Nodes Prices Parameter enforcement

— Capacity License: CISCO-ASR9000 #Nodes Price Parameter enforcement

— Capacity License: CISCO-ASR900 #Nodes Price Parameter enforcement

— Capacity License: JUNIPER-MX #Nodes Price Parameter enforcement

— Capacity License: JUNIPER-PTX #Nodes Price Parameter enforcement

— Capacity License: JUNIPER-SRX #Nodes Price Parameter enforcement

— Capacity License: JUNIPER-vSRX #Nodes Price Parameter enforcement

— Capacity License: JUNIPER-vMX #Nodes Price Parameter enforcement

7.16.3 License Alarm

When the license is close to expiry or has expired or close to or at full capacity, a license alarm is displayed in the FM GUI. The license alarm threshold can be set in the CLI, refer to the online help for details.

The alarm severities are as follows:

— Threshold related alarms -> WARNING

— License expired alarm -> CRITICAL

— In enforcement alarm -> CRITICAL

— In GP alarm -> MAJOR

— In EU alarm -> MAJOR

— EU exhausted alarm -> MAJOR

7.16.4 Activate System Emergency Unlock

Description

This LCM command allows an ENM system administrator to activate the system emergency unlock.

During emergency unlock, license blocking actions related to any function in ENM do not take place, irrespective of the resource usage or license installation. The default duration for the emergency unlock is 7 days, and the number of activations allowed is 2. The activation of emergency unlock raises an alarm.

To reactivate the emergency unlock you must order an Emergency Unlock Reset Key via the Ericsson Support Organization.

The installation of the key will reset the number of activations from 2 to 0. The end of the emergency unlock procedure is rounded to the end of day.

Steps

1. Activate the emergency unlock.

   ```
   lcmadm activate --emergency-unlock
   ```

   Example

   ```
   lcmadm activate --emergency-unlock
   Emergency unlock successfully activated
   ```

2. Check the emergency unlock activated time, duration, and usage.

   ```
   lcmadm get -eui
   ```

   The system returns the following output:

Example

```
lcmadm get -eui
Emergency Unlock Info
Allowed Activation Limit      Usage   Status  Duration (days)  Date →
 Activated
2                             1       Active  7                  N →
ov 09 2016 13:19:33 GMT
```

7.16.5 Add New ENM Licenses

This LCM command allows an ENM system administrator to add new ENM licenses to the system.

```
lcmadm install file:<license-file-name>
```

Where:

— <license-file-name> is the file that contains the ENM licenses.

```
lcmadm install file:<license-file-name>
```

This task describes how to add new licenses in the `licenses.txt` file.

Steps

1. Drag and drop the `licenses.txt` file into the ENM CLI console
2. Enter the following command

```
lcmadm install file:licenses.txt
1 license(s) successfully installed.
```

7.16.6 Export Current License Usage

This LCM command allows an ENM system administrator to export current license usage and save it to a file on a local client machine.

```
lcmadm export (--current-usage | -cu)
```

Steps

1. Enter the following command to export the current license usage:

```
lcmadm export -cu
```

2. Follow the instructions on the browser to save the license usage file on the local machine.

7.16.7 Export Historical License Usage

This LCM command allows an ENM system administrator to export historical license usage and save it as a file on a local client machine.

```
lcmadm export (--historical-usage | -hu)=<days>
```

where <days> is range of the historical report. Valid values are 7, 30, 90, or 180.

Steps

1. Enter the following command to export the historical license usage for the past seven days.

   ```
   lcmadm export -hu=7
   ```

2. Follow the instructions on the browser to save the license usage file on the local machine.

7.16.8 List Installed Licenses

This LCM command allows an ENM system administrator to list both the installed license information and the current license usage information.

```
lcmadm list
```

Steps

1. Enter the following command to list information for all installed licenses:

   ```
   lcmadm list
   ```

   Example

   ```
   lcmadm list

   Feature Licenses
   License Name            Expiry Date                          Vendor Info
   LTEMgr License1         Dec 31 2015 00:00:00 IST             Vendor1
   LTEMgr License2         Dec 31 2015 00:00:00 IST (expired)   Vendor2

   Capacity License
   License Name            Expiry Date                          Limit   Vendor Info
   eNodeB License1         Dec 31 2015 00:00:00 IST             100     Vendor1
   eNodeB License2         Dec 31 2015 00:00:00 IST (expired)   200     Vendor2
   ```

7.16.9 List Installed License Usage

This LCM command allows an ENM system administrator to list the usage information for all currently installed licenses.

```
lcmadm list (--current-usage | -cu)
```

Steps

1. Enter the following command to list usage information for all currently installed licenses:

   ```
   lcmadm list -cu
   ```

   Example

   ```
   lcmadm list -cu
   Capacity License
   License Name            Expiry Date                              Limit   Usag →
   e   Vendor Info
   eNodeB License1         Dec 31 2015 00:00:00 IST                 100     10   →
       Vendor1
   eNodeB License2         Dec 31 2015 00:00:00 IST (expired)       200     120  →
       Vendor2
   ```

7.16.10 Query Grace Period Information

This LCM command allows an ENM system administrator to list the grace period information for all installed licenses.

```
lcmadm get (--grace-period-info | -gpi)
```

where <license-name> is the license name or license ID.

The system default duration for the grace period is 14 days. The end of the grace period duration is rounded to the end of day.

Steps

1. Enter the following command to query the grace period information for all installed licenses

   ```
   lcmadm get -gpi
   ```

   Example

   ```
   lcmadm get -gpi

   License Name            Status                          Duration (days)         Date Ac →
   tivated                          Base Limit for GP Renewal
   ```

```
eNodeB License1            Grace Period Available          14                      N/A
                                 N/A
eNodeB License2         In Grace Period                 14                      Feb 02
2015 11:37:25 IST               100
eNodeB License3            Grace Period Used               14                      N/A
                                 100
eNodeB License4            License Expired                 N/A                     N/A
                                 N/A
XYZ License             Grace Period Not Applicable     N/A                     N/A
                                N/A
```

7.16.11 Query License Alarm Threshold Information

This LCM command allows an ENM system administrator to list the following threshold information for all installed licenses:

— License expiry threshold

— License capacity threshold

```
lcmadm get [name=<license-name>] (--threshold | -t)
```

where <license-name> is the license name or license ID.

Steps

1. Enter the following command to query license threshold information for all installed licenses:

```
lcmadm get -t

License Name    Expiry Threshold (days)         Capacity Threshold (percentage)      Ve
ndor Info
Sample2         30                              90                                   Ve
ndor1
Sample3         30                              90                                   Ve
ndor2
```

2. Enter the following command to query license threshold information for the `Sample2` license:

```
lcmadm get name=Sample2 -t
License Name    Expiry Threshold (days)         Capacity Threshold (percentage)    Vend
or Info
Sample2         30                              90                                 Vend
or1
```

7.16.12 Query License Emergency Unlock Information

This LCM command allows an ENM system administrator to show the system emergency unlock status.

```
lcmadm get (--emergency-unlock-info | -eui)
```

Steps

1. Enter the following command to query the ENM system emergency unlock status:

```
lcmadm get -eui
```

Example

```
lcmadm get -eui
Emergency Unlock Info
Allowed Activation Limit      Usage   Status  Duration (days)  Date Activated
2                             1       Active  7                     Nov 09 2016 13:19 →
:33 GMT
```

7.16.13 Remove Existing Licenses

This LCM command allows an ENM system administrator to remove an existing ENM license from the system.

```
lcmadm remove name=<license-name>
```

where <license-name> is the license name or license ID

Steps

1. Enter the following command to remove the `FAT1023105` license from the ENM system:

```
lcmadm remove name=FAT1023105
License successfully removed.
```

Note: The above command removes the license from the Sentinel license table. There is a known limitation for removing licenses completely from the Sentinel license file. To also remove a license from this file, perform the following workaround:

a. Log into LMS on Physical deployment or Sentinel VM on Cloud deployment.

b. Edit the `opt/SentinelRMSSDK/licenses/lservrc` file, and remove the line containing the specific license feature that is no longer wanted.

c. Save the file.

7.16.14 Set License Capacity Threshold

This LCM command allows an ENM system administrator to change the license capacity threshold percentage value for a given installed license.

```
lcmadm set name=<license-name> (--capacity-threshold | -ct) = <percentage>
```

Where:

— <license-name> is the license name or license ID, and

— <percentage> is the new capacity threshold value as a percentage.

Steps

1. Enter the following command to change the license capacity threshold for the `Sample2` license from its current value to 85%

```
lcmadm set name="Sample2" -ct=85
Capacity threshold successfully updated
```

7.16.15 Set License Expiry Threshold

This LCM command allows an ENM system administrator to change the license expiry threshold days for a given installed license.

```
lcmadm set name=<license-name> (--expiry-threshold | -et) = <days>
```

Where:

— <license-name> is the license name or license ID.

— <days> is new expiry threshold value in days.

Steps

1. Enter the following command to change the license expiry threshold for the `Sample2` license from its current value to 60 (days):

```
lcmadm set name="Sample2" -et=60
Expiry threshold successfully updated
```

7.16.16 Query Capacity License Enforcement Info

Command `lcmadm get --enforcement-info` lists the capacity licenses which are in enforcement. The “Base limit for Enforcement clearing“ uses the limit recorded when GP gets started.

```
lcmadm get (--capacity-enforcement-info| -cei)
```

Steps

1. Run the following command.

```
lcmadm get -cei

License Name            Date Triggered                  Base Limit for GP Renewal
eNodeB License1            Feb 02 2015 11:37:25 IST        100                          →
```

7.17 PostgreSQL Database Administration Tasks

The information in this section refers to PostgreSQL installations in ENM.

Prerequisites

Root access is required for `postgres_admin.sh`

Note: The only authorized ways for administering or troubleshooting PostgreSQL is by using the PostgresSQL Admin Utility, or using procedures defined herein. Access to PostgreSQL Databases via "PSQL" or any 3rd Party applications is prohibited, and may result in data loss. Usage of other features or methods to run any operations, monitoring procedures, or activities on data managed by the PostgreSQL service is prohibited. If there are any features needed that are not provided and documented herein then contact Ericsson Support.

PostgreSQL Admin

A general information/server status script is available in `/opt/ericsson/pgsql/util/postgres_admin.sh` where postgres is installed.

The `postgres_admin.sh` script offers an interactive menu for querying the ENM PostgreSQL Service and PostgreSQL Application Database for information on ENM.

This can be used as a troubleshooting/general information utility.

```
*************************************************************

      ENM - PostgreSQL DBA Utility

      Date: Mon Mar  4 12:06:23 GMT 2019
*************************************************************

      Select the action you want to perform:

             1. Version & Key File Locations
```

```
 2. Uptime
 3. Non Default Configuration Parameters
 4. Database User List & Privileges
 5. Database List / Space Used
 6. Database Table Space Listing
 7. Database Table Row Listing
 8. Current Running Process Listing
 9. Server Level Longest running transactions
10. DB Level Current Longest Running Transactions
11. DB Resource Usage
12. PostgreSQL Connectivity Audit Logging
13. PostgreSQL Role's Expiration Period
14. PostgreSQL Database Space Maintenance Options
15. PostgreSQL File System Monitor
 0. Exit


Enter your choice [1-15 or 0 to exit]:
```

Alternatively, the `postgres_admin.sh` script can be executed without the menu by using the following optional parameters:

```
/opt/ericsson/pgsql/util/postgres_admin.sh -V -U -C -P -S -s -r -t -x -X -c -A -
E -M -R -H
```

Table 30 Arguments Detail

-V	Postgres Version Report
-U	Uptime Report
-C	Non-Default Configuration Report
-P	Login Privileges
-S	Space Usage
-s	Database Table Size
-r	Database Table Row Listing
-t	Running Transactions
-x	Server Level Longest Running Transactions (20)
-X	Database Level Longest Running Transactions (20)
-c	Resource Characteristics
-A	PostgreSQL Connectivity Audit Logging
-E	Remove Postgres Role Expiry
-M	Database Space Table Maintenance
-R	File System Monitor
-H	Help

PostgreSQL Directory Structure

PostgreSQL server is installed on `/ericsson/postgres`. This directory stores all of the PostgreSQL server configuration files and non-user-modifiable files.

PostgreSQL server is initialized on `/ericsson/postgres/data` where PostgreSQL is running.

PostgreSQL server configuration files and database data files can be found under `/ericsson/postgres/data` on the active DB node.

Note: Changing the directory is not recommended as this can cause an unrecoverable error with PostgreSQL.

Generic PostgreSQL utilities are installed in `/opt/rh/rh-postgresql94/root/usr/bin`.

PostgreSQL Postgres User Password and Connectivity

The default superuser Postgres (not POSIX user) requires a password to open a connection.

You can open a CLI connection to Postgresql as the Postgres DB user from the host where postrgres is running as shown in the following example:

```
su - postgres -c "PGPASSWORD=password /opt/rh/postgresql/bin/psql -U postgres -h
 postgresql01"
```

Note: The password can be found in the SED, matching the `postgresql01_admin_password` parameter.

PostgreSQL Logging

The log file is rotated when the file size reaches 1GB or if seven days have passed since the last rotation. PostgreSQL is configured to log the following type of messages: ERROR, LOG, FATAL, and PANIC.

Note: For information about PostgreSQL logging, refer to the section *If Issue Suspected on PostgreSQL Database* in the *ENM Data Collection Guidelines*. This is available from Local Ericsson Support.

PostgreSQL Modeled Parameters

Note: This details in the following document are provided for information purposes only. These parameters should not be changed.

For more information on PostgreSQL, see: http://www.postgresql.org/docs/

7.17.1 PostgreSQL Connectivity Audit Logging

Option 12 of the Postgres Admin Tool allows the user to enable PostgreSQL connection logging. By selecting this option, all connections/disconnections and their duration can be logged. It also provides a view to failed PostgreSQL Connections.

From the Main menu of the Postgres Admin tool, select Option 12:

```
*************************************************************
      ENM - PostgreSQL DBA Utility

      Date: Wed Jun  6 15:11:30 IST 2018
*************************************************************

      Select the action you want to perform:

             1. Version & Key File Locations
             2. Uptime
             3. Non Default Configuration Parameters
             4. Database User List & Privileges
             5. Database List / Space Used
             6. Database Table Space Listing
             7. Database Table Row Listing
             8. Current Running Process Listing
             9. Server Level Longest running transactions
            10. DB Level Current Longest Running Transactions
            11. DB Resource Usage
            12. PostgreSQL Connectivity Audit Logging
            13. Postgres Role's Expiration Period
             0. Exit

      Enter your choice [1-13 or 0 to exit]:
```

Connectivity Audit Logging

The user is presented with the PostgreSQL Audit Logging sub-menu. From this menu, the user can enable/disable Connectivity Audit Logging. The user can also view failed connections.

Select Option 1 to enable the connectivity audit logging:

```
            *************************************************************
            PostgreSQL Connectivity Audit Logging
            *************************************************************
            ENABLE/DISABLE Connectivity Audit Logging
            All connections, associated disconnections and connectivity duration will be logged.
            Logs can be found in /var/log/messages or via ENM LogViewer.
            Failed Connections
            Display Failed Connections from 12:00am Today.
            Display Failed Connections prior to Today.
            A restart of PostgreSQL service will be required to ENABLE/DISABLE Connectivity Audit →
Logging.
            1) Enable Connectivity Audit Logging
            2) Disable Connectivity Audit Logging
            3) Display Failed Connections from 12:00am Today
            4) Display Failed Connections prior to Today
            5) Quit
            Please make a choice or press enter:1
```

Note: A restart of the PostgreSQL service will occur.

Selecting Option 1 from the PostgreSQL Audit Logging sub-menu will enable the Connectivity Audit Logging and the following output is displayed:

```
            ========================================================================
            Connectivity Audit Logging
            Enabling Connectivity Audit Logging
            ========================================================================
            postgres_failed_authentications_audit: [DEBUG]: /opt/ericsson/pgsql/etc/litp_base.conf →
 is on this Node. Continuing...
            postgres_failed_authentications_audit: [DEBUG]: PostgreSQL service is running on this →
Database Node.
            postgres_failed_authentications_audit: [INFO]: Config Enabled:: log_duration
            postgres_failed_authentications_audit: [INFO]: Config Enabled:: log_connections
            postgres_failed_authentications_audit: [INFO]: Config Enabled:: log_line_prefix
            postgres_failed_authentications_audit: [INFO]: Config Enabled:: log_disconnections
            postgres_connectivity_audit: [INFO]: Attempting to restart the service PostgreSQL
            Postgres LSB rh-postgresql94: INFO: Service Stopped
            Postgres LSB rh-postgresql94: INFO: Attempting to start PostgreSQL
            Postgres LSB rh-postgresql94: INFO: Service Started
            postgres_connectivity_audit: [INFO]: PostgreSQL service was successfully restarted.
            postgres_failed_authentications_audit: [INFO]: Successfully Added Cronjob: /etc/cron.d →
/audit_log_cron_warning.sh
            postgres_failed_authentications_audit: [INFO]: Successfully Added Cronjob: /etc/cron.d →
/auto_disable_audit_log.sh
            postgres_failed_authentications_audit: [INFO]: PostgreSQL Connectivity Audit Logging i →
s now enabled.
            postgres_failed_authentications_audit: [WARNING]: Please DISABLE the PostgreSQL Connec →
tivity Audit Logging as soon as the Audit is Over.
```

Logs can be viewed on the host where PostgreSQL is active in /var/log/messages and also via ENM LogViewer.

```
            [root@cloud-db-1 ~]# tail -f /var/log/messages
            May 8 16:03:47 cloud-db-1 postgresql01[29593]: [2293-1] db=openidm,user=openidm,host=1 →
0.247.246.122,SELECTLOG: duration: 0.213 ms
            May 8 16:03:47 cloud-db-1 postgresql01[29595]: [1939-1] db=openidm,user=openidm,host=1 →
0.247.246.122,PARSELOG: duration: 0.072 ms
            May 8 16:03:47 cloud-db-1 postgresql01[29595]: [1940-1] db=openidm,user=openidm,host=1 →
0.247.246.122,BINDLOG: duration: 0.556 ms
            May 8 16:03:47 cloud-db-1 postgresql01[29595]: [1941-1] db=openidm,user=openidm,host=1 →
0.247.246.122,SELECTLOG: duration: 0.041 ms
            May 8 16:03:47 cloud-db-1 postgresql01[29594]: [2050-1] db=openidm,user=openidm,host=1 →
0.247.246.122,PARSELOG: duration: 0.024 ms
            May 8 16:03:47 cloud-db-1 postgresql01[29594]: [2051-1] db=openidm,user=openidm,host=1 →
0.247.246.122,BINDLOG: duration: 0.007 ms
            May 8 16:03:47 cloud-db-1 postgresql01[29594]: [2052-1] db=openidm,user=openidm,host=1 →
0.247.246.122,SHOWLOG: duration: 0.009 ms
            May 8 16:03:47 cloud-db-1 postgresql01[29594]: [2053-1] db=openidm,user=openidm,host=1 →
0.247.246.122,PARSELOG: duration: 0.016 ms
            May 8 16:03:47 cloud-db-1 postgresql01[29594]: [2054-1] db=openidm,user=openidm,host=1 →
0.247.246.122,BINDLOG: duration: 0.005 ms
            May 8 16:03:47 cloud-db-1 postgresql01[29594]: [2055-1] db=openidm,user=openidm,host=1 →
0.247.246.122,SETLOG: duration: 0.006 ms
```

After approximately 2 hours, the Connectivity Audit Logging is auto disabled.

To Manually disable the Connectivity Audit Logging, select option 2 from the PostgreSQL Audit Logging sub-menu:

Note: A restart of the PostgreSQL service will occur.

```
            1) Enable Connectivity Audit Logging
            2) Disable Connectivity Audit Logging
```

```
            3) Display Failed Connections from 12:00am Today
            4) Display Failed Connections prior to Today
            5) Quit
            Please make a choice or press enter:2
```

Selecting Option 2 from the PostgreSQL Audit Logging sub-menu will disable the Connectivity Audit Logging and the following output is displayed:

```
            ================================================================================
            Connectivity Audit Logging
            Disabling Connectivity Audit Logging
            ================================================================================
            postgres_failed_authentications_audit: [DEBUG]: /opt/ericsson/pgsql/etc/litp_base.conf  →
 is on this Node. Continuing...
            postgres_failed_authentications_audit: [INFO]: Config Reverted:: log_duration
            postgres_failed_authentications_audit: [INFO]: Config Reverted:: log_connections
            postgres_failed_authentications_audit: [INFO]: Config Reverted:: log_line_prefix
            postgres_failed_authentications_audit: [INFO]: Config Reverted:: log_disconnections
            postgres_connectivity_audit: [INFO]: Attempting to restart the service PostgreSQL
            Postgres LSB rh-postgresql94: INFO: Service Stopped
            Postgres LSB rh-postgresql94: INFO: Attempting to start PostgreSQL
            Postgres LSB rh-postgresql94: INFO: Service Started
            postgres_connectivity_audit: [INFO]: PostgreSQL service was successfully restarted.
            postgres_failed_authentications_audit: [INFO]: Successfully removed cronjob: /etc/cron  →
.d/audit_log_cron_warning.sh
            postgres_failed_authentications_audit: [INFO]: Successfully removed cronjob: /etc/cron  →
.d/auto_disable_audit_log.sh
            postgres_failed_authentications_audit: [INFO]: PostgreSQL Connectivity Audit Logging h  →
as been Disabled.
```

Failed Connections

Selecting Option 3 from the PostgreSQL Audit Logging sub-menu will display Today's Failed Connections. All failed connections from 12.00 am Today until current time will be displayed.

```
            1) Enable Connectivity Audit Logging
            2) Disable Connectivity Audit Logging
            3) Display Failed Connections from 12:00am Today
            4) Display Failed Connections prior to Today
            5) Quit
            Please make a choice or press enter:3
```

If no failed connections occurred Today, an example output of this option would be as follows:

```
            ================================================================================
            PostgreSQL Failed Connection Audit Log
            Failed Connections from 12:00am Today
            ================================================================================
            Today's Failed Connections:
            No Failed Connections Today
```

The following is an example of a failed connection due to an incorrect password:

```
            su - postgres -c "PGPASSWORD=wrong_password /opt/rh/postgresql/bin/psql -U postgres -h  →
```

```
 postgresql01 -c '\l'"
```

If the above failed connection occurred Today, the output of this option would be as follows:

```
            ================================================================================
            PostgreSQL Failed Connection Audit Log
            Failed Connections from 12:00am Today
            ================================================================================
            Today's Failed Connections:
            # 1: 2018-05-04T14:52:26.419007+01:00:  [3-1] db=postgres,user=postgres,authentication  →
FATAL:  password authentication failed for user "postgres"
            Please make a choice or press enter:
```

Selecting Option 4 from the PostgreSQL Audit Logging sub-menu will display all previously failed connections prior to Today.

```
            1) Enable Connectivity Audit Logging
            2) Disable Connectivity Audit Logging
            3) Display Failed Connections from 12:00am Today
            4) Display Failed Connections prior to Today
            5) Quit
            Please make a choice or press enter:4
```

An example output for all previously failed connections prior to Today:

```
            ================================================================================
            PostgreSQL Failed Connection Audit Log
            Output from /ericsson/postgres/data/postgres_failed_connection_audit_log
            ================================================================================
            All Failed Connections:
            2018.05.01  No Failed Connections
            2018-05-02T17:37:27.332339+01:00:  [3-1] db=fls,user=fls,authenticationFATAL:  no pg_h  →
ba.conf entry for host "10.247.244.3", user "fls", database "fls", SSL off
            2018-05-02T17:37:27.330616+01:00:  [3-1] db=fls,user=fls,authenticationFATAL:  no pg_h  →
ba.conf entry for host "10.247.244.3", user "fls", database "fls", SSL on
            2018-05-02T17:37:08.607940+01:00:  [3-1] db=invalid_user,user=invalid_user,authenticat  →
ionFATAL:  no pg_hba.conf entry for host "10.247.244.3", user "invalid_user", database "invalid_us  →
er", SSL off
            2018-05-02T17:37:08.605886+01:00:  [3-1] db=invalid_user,user=invalid_user,authenticat  →
ionFATAL:  no pg_hba.conf entry for host "10.247.244.3", user "invalid_user", database "invalid_us  →
er", SSL on
            2018-05-02T17:36:27.099900+01:00:  [3-1] db=postgres,user=postgres,authenticationFATAL  →
:  password authentication failed for user "postgres"
            2018-05-02T17:36:27.097502+01:00:  [3-1] db=postgres,user=postgres,authenticationFATAL  →
:  password authentication failed for user "postgres"
            2018-05-03T11:59:30.375696+01:00:  [3-1] db=invalid_user,user=invalid_user,authenticat  →
ionFATAL:  no pg_hba.conf entry for host "10.247.244.3", user "invalid_user", database "invalid_us  →
er", SSL off
            2018-05-03T11:59:30.373146+01:00:  [3-1] db=invalid_user,user=invalid_user,authenticat  →
ionFATAL:  no pg_hba.conf entry for host "10.247.244.3", user "invalid_user", database "invalid_us  →
er", SSL on
```

Selecting Option 5 from the PostgreSQL Audit Logging sub-menu, followed by the return key will exit back to the main menu.

```
            Please make a choice or press enter:
            1) Enable Connectivity Audit Logging
            2) Disable Connectivity Audit Logging
```

```
            3) Display Failed Connections from 12:00am Today
            4) Display Failed Connections prior to Today
            5) Quit
            Please make a choice or press enter:5
            Press <Return> to continue:
```

7.17.2 Check the Database Administrator Password Expiration Period for PostgreSQL

A validation period can be set on a new or existing password. If the expiration period expires, connections to the PostgreSQL databases are blocked. To recover from this scenario, please refer to Recover from Database Administrator Password Expiring for PostgreSQL.

Prerequisites

Root access to host where Postgres is running.

Steps

1. Execute the PostgreSQL DBA Utility

```
root@ # /opt/ericsson/pgsql/util/postgres_admin.sh
```

2. Select **`Option 13`**:

```
*************************************************************
      ENM - PostgreSQL DBA Utility

      Date: Wed Jun  6 15:11:30 IST 2018
*************************************************************

      Select the action you want to perform:

             1. Version & Key File Locations
             2. Uptime
             3. Non Default Configuration Parameters
             4. Database User List & Privileges
             5. Database List / Space Used
             6. Database Table Space Listing
             7. Database Table Row Listing
             8. Current Running Process Listing
             9. Server Level Longest running transactions
            10. DB Level Current Longest Running Transactions
            11. DB Resource Usage
            12. PostgreSQL Connectivity Audit Logging
            13. Postgres Role's Expiration Period
             0. Exit

      Enter your choice [1-13 or 0 to exit]:
```

3. Select **`Option 1`** - Check Postgres role expiry

```
*************************************************************
          Postgres Role's Expiration Period
*************************************************************


1) Check postgres role expiry    3) Quit
```

```
2) Disable postgres role expiry
Please make a choice or press enter:1
```

Sample Output:

```
================================================================================
                        Connectivity Audit Logging

                        Check postgres role expiry
================================================================================

postgres_expiry_checker: [DEBUG]: postgresql01 is accepting connections.
postgres_expiry_checker: [INFO]: Postgres role validity has 45 days until ex →
piry.
```

4. To exit the script enter **<3>**, **<enter>**, **<0>**, followed by **<enter>**.

7.17.3 Monitor the Database Administrator Password Expiration for PostgreSQL

Note: To manually check the Expiry period, refer to Check the Database Administrator Password Expiration Period for PostgreSQL.

At 3 a.m., a daily task executes to check how many days are left until the Database Administrator Password for PostgreSQL expires.

A log message is created, with 3 potential log levels:

Days remaining before expiry	Log Level	Message
2 Days or less	Error	postgres_expiry_checker: [ERROR]: Postgres role validity has 2 day(s) until expiry.
3 Days and less than 10 days	Warning	postgres_expiry_checker: [WARNING]: Postgres role validity has 5 days until expiry. postgres_expiry_checker: [WARNING]: To alter the validation period for the Postgres role refer to ENM System Admin Guide
Greater than 10 days	Info	postgres_expiry_checker: [INFO]: Postgres role validity has 45 days until expiry.

Prerequisites

Root access to Database Nodes (DB).

Steps

1. Log on to <DB-node> as the litp-admin user and switch to the root user.

   Refer to Log On to Active PostgreSQL DB Node.

2. Check the `/var/log/messages`.

```
[root@<db-node> ~]# grep -i "postgres_expiry_checker" /var/log/messages
```

Sample Output:

```
[root@cloud-db-1 ~]# grep -i "postgres_expiry_checker" /var/log/messages
Jun  6 03:00:02 cloud-db-1 postgres_expiry_checker: [DEBUG]: postgresql01 is
 accepting connections.
Jun  6 03:00:02 cloud-db-1 postgres_expiry_checker: [INFO]: Postgres role va
lidity has 45 days until expiry.
```

7.17.4 Recover from Database Administrator Password Expiring for PostgreSQL

How to recover from a scenario where the Database Administrator password has expired for PostgreSQL. By executing this functionality, the Database Administrator password expiration period is set to infinity.

Prerequisites

Root access to Database Nodes (DB).

Steps

1. Log on to <DB-node> as the litp-admin user and switch to the root user.
2. Execute the remove_role_expiry.sh script:

```
[root@<db-node> ~]# /opt/ericsson/pgsql/util/remove_role_expiry.sh
```

Sample Output:

```
postgres_pass_expiry: [INFO]: Attempting to remove Postgres role's validity
period.
postgres_pass_expiry: [INFO]: Successfully removed Postgres role's validity
period.

To add a validation period for the Postgres role refer to ENM System Admin G
uide -1/1543-AOM 901 151
```

Note: The validation period for the password is reset to infinity. To set a validation period for the Database Administrator Password Expiration Period for PostgreSQL, refer to Change the Database Administrator Password Expiration Period for PostgreSQL.

7.17.5 Change the Database Administrator Password for PostgreSQL

> How a root user can change the Database Administrator password for PostgreSQL, and set an expiration period for the password.

Follow these steps to change the default password:

— After initial installation

— If the PostgreSQL password has been compromised.

— When the PostgreSQL password is about to expire.

The script can be only be called from Management Server (MS).

Note: Change "`postgresql01_admin_password`" in the *Site Engineering Document* to reflect the new password as the change affects subsequent ENM upgrades.

A validation period can be set on a new or existing password. If the expiration period expires, connections to the PostgreSQL databases are blocked. To recover from this scenario, refer to Recover from Database Administrator Password Expiring for PostgreSQL.

Prerequisites

— Root access to Management Server (ms-1), the DB Cluster (db-) and the Service Cluster (svc). The latter 2 are used for validation.

— The *Site Engineering Document* is available for updates.

— Keep a separate note of the new password, as it will be required prior to an upgrade. This is because the current Site Engineering Document may be replaced.

— The new password must be manually added to the new *Site Engineering Document* pre-upgrade.

Steps

1. Log on to the ENM MS-1 as the `litp-admin` user and switch to the `root` user.

   Take a note of the current Database Administrator password (MD5 Hashed) as follows:

   ```
   [root@<ms> tmp]#cat /ericsson/tor/data/global.properties | grep postgresql01 →
   _admin_password=
   ```

2. Run the following script to change the PostgreSQL Database Administrator password and expiration period:

   ```
   [root@<ms> tmp]#/opt/ericsson/postgresql/change_postgresql_password.sh
   ```

   The script outputs the following:

   ```
   ========================================================================== →
   ===========
   ```

```
Script to change postgresql01_admin_password - monitor /var/log/messages for
 status
================================================================================
==========
This script will automatically via LITP update global.properties
Postgresql Password Change will amend LITP Model and run a new plan with 2 c
hange tasks
Do not run this script in parallel with any ongoing LITP Plan Changes
================================================================================
==========
Are you sure that you want to change the Postgresql password? (y/n)
```

3. Enter the current PostgreSQL Database Administrator password when prompted.

```
Choice confirmed to proceed with password change

      Please provide current password:
```

4. Enter a new password that complies with the following criteria:

```
Please provide new password:
```

   — The password must have at least eight characters.

   — The password must contain at least 1 lower case alpha character.

   — The password must contain at least 1 upper case alpha character.

   — The password must contain at least 1 numeric character.

   — The password must not contain: username, first name, or surname.

   — The password may contain special characters (non-alphanumeric characters).

     However, only hyphen (-) , underscore (_), and period (.) are allowed in the password.

5. Repeat the new password.

```
Please repeat new password:
```

6. Enter **y** to confirm the password change.

```
Passwords are given properly.
      Are you sure, you want to change password? (y/n)
```

   Result: The new password will be confirmed:

```
y
A new Password is confirmed
```

7. This creates an LITP Plan, and the plan executes automatically. This updates the Global Properties with the new (MD5 Hashed) password.

Note: This task will loop for several minutes until both tasks are completed.

```
================================================================================ →
===========
Please wait for LITP associated tasks to be created(LITP create_plan)
This may take several minutes
Checking ongoing LITP Model Operations and status of Previous Plan
================================================================================ →
===========
Previous LITP Plan successful and no plan ongoing - proceed
================================================================================ →
===========
Running LITP Updates of Global Properties
================================================================================ →
===========
Running LITP create plan to update modelled properties for Postgresql Passwo →
rd
LITP Create Plan is running:
================================================================================ →
===========
Phase 1
    Task status
    -----------
    Initial     /ms/items/config_manager
            Install/Update config_manager

Tasks: 1 | Initial: 1 | Running: 0 | Success: 0 | Failed: 0 | Stopped: 0
Plan Status: Initial
Phase 1
    Task status
    -----------
    Initial     /ms/items/config_manager
            Install/Update config_manager

Tasks: 1 | Initial: 1 | Running: 0 | Success: 0 | Failed: 0 | Stopped: 0
Plan Status: Initial
```

8. Once the LITP Plan is successful, the user is prompted with an option to set the password expiry:

```
================================================================================ →
===========
Confirm if the password expiry shall be set for user postgres
================================================================================ →
===========
Are you sure that you want to set the password expiry? (y/n)
```

9. Enter **y** to add an Expiry Period.

   Note: Password Expiry:

   When the user is prompted to set the expiry, if **n** is selected, the password expiry is set to infinity. This means the Database Administrator password will not expire.

   The user will enter an integer value for the number of days of the expiry period.

```
Choice confirmed to proceed with postgres user password expiry
Enter the postgres user password expiry in days
```

   As an example, the user enters **45**. This sets the password to expire in 45 days from the current date. The following is an example output:

```
========================================================================== →
==========
            The expiry for user postgres was set
            ============================================================== →
======================
            Altering the postgres user with new password
            ============================================================== →
======================
            Phase 1
            Task status
            -----------
            Success     /ms/items/config_manager
            Install/Update config_manager

            Tasks: 1 | Initial: 0 | Running: 0 | Success: 1 | Failed: 0 | St →
opped: 0
            Plan Status: Successful
            ============================================================== →
======================
            The New Postgres DBA Password is Validated
            ============================================================== →
======================
```

Results

On completion, the Database Administrator password is updated in PostgreSQL and the corresponding MD5 hash (postgresql01_admin_password) is updated in the `global.properties` file.

7.17.6 Disable Database Administrator Password Expiration Period for PostgreSQL

How to disable the Database Administrator password expiration period for PostgreSQL. By executing this functionality, the Database Administrator password expiration period is set to infinity.

A validation period can be set on a new or existing password. If the expiration period expires, connections to the PostgreSQL databases are blocked. To recover from this scenario, refer to Recover from Database Administrator Password Expiring for PostgreSQL.

Note: This section is for removing an expiration period on an existing Postgres password. To recover from an expired Postgres password, refer to Recover from Database Administrator Password Expiring for PostgreSQL.

To set a validation period for the Database Administrator Password Expiration Period for PostgreSQL, refer to Change the Database Administrator Password Expiration Period for PostgreSQL.

Prerequisites

Root access to the Database Nodes (DB).

Steps

1. Log on to the <db-node> as the litp-admin user and switch to the root user.

2. Execute the PostgreSQL DBA Utility:

```
[root@<db-node> ~]# /opt/ericsson/pgsql/util/postgres_admin.sh
```

3. Select **Option 13**:

```
***************************************************************
      ENM - PostgreSQL DBA Utility

      Date: Wed Jun  6 15:11:30 IST 2018
***************************************************************

      Select the action you want to perform:

             1. Version & Key File Locations
             2. Uptime
             3. Non Default Configuration Parameters
             4. Database User List & Privileges
             5. Database List / Space Used
             6. Database Table Space Listing
             7. Database Table Row Listing
             8. Current Running Process Listing
             9. Server Level Longest running transactions
            10. DB Level Current Longest Running Transactions
            11. DB Resource Usage
            12. PostgreSQL Connectivity Audit Logging
            13. Postgres Role's Expiration Period
             0. Exit

      Enter your choice [1-13 or 0 to exit]:
```

4. Select **Option 2** - Disable Postgres role expiry

```
Select Option 2 - Disable Postgres role expiry
```

5. Select **Option 1** - Remove Postgres Role's Expiry

```
================================================================================
                      Connectivity Audit Logging

                    Disable postgres role expiry
================================================================================

Remove Postgres Role's Expiry.
Only use this feature, when the Postgres Role has expired.

1) Remove Postgres Role's Expiry
2) Return to previous menu
```

The Database Administrator password expiration period is set to infinity.

Sample Output:

```
================================================================================
                       Remove Postgres Role's Expiry
================================================================================

postgres_pass_expiry: [INFO]: Attempting to remove Postgres role's validity  →
period.
postgres_pass_expiry: [INFO]: Successfully removed Postgres role's validity  →
period.

To add a validation period for the Postgres role refer to ENM System Admin G →
uide -1/1543-AOM 901 151
```

6. To exit the script enter **<2>**, **<enter>**, **<3>**, **<enter>**,**<0>**, followed by **<enter>**.

7.17.6.1 Remove Expiry Period via Optional Argument

Instead of using the PostgreSQL DBA Utility interactive menu, the script can be executed by passing the optional argument -E. The -E optional argument will remove the Postgres Role's expiry period, setting the expiration period to infinity.

```
[root@<DB-node> ~]# /opt/ericsson/pgsql/util/postgres_admin.sh -E
```

Sample Output:

```
================================================================================
                        Remove Postgres Role's Expiry
================================================================================

postgres_pass_expiry: [INFO]: Attempting to remove Postgres role's validity peri →
od.
postgres_pass_expiry: [INFO]: Successfully removed Postgres role's validity peri →
od.

To add a validation period for the Postgres role refer to ENM System Admin Guide →
 -1/1543-AOM 901 151
```

7.17.7 Create a Dump/Backup of the PostgreSQL Database

> This task describes the steps to create an sql dump of a PostgreSQL database.

Prerequisites

— Root access to the host where postgres is running.

Steps

1. Log on to the host where postgres is running, switch to the root user and then switch to postgres user.
2. Change to the PostgreSQL `bin` directory.

   ```
   [-bash-4.1$] cd /opt/rh/rh-postgresql94/root/usr/bin
   ```

3. List the databases using `psql`.

   ```
   [-bash-4.1$] ./psql -l
   ```

4. Run the following query to get the size of the database to be backed up

```
[-bash-4.1$] ./psql
[postgres=#] SELECT pg_size_pretty(pg_database_size('<db_name>'));
```

Example

```
[postgres=#] SELECT pg_size_pretty(pg_database_size('wfsdb'));
```

Example output:

```
pg_size_pretty
----------------
9165 kB
```

The space displayed is the databases' current used space. The database backup file will be significantly less than the used space displayed.

As a rule of thumb, ensure there is at least 50% of the used space available for the associated backup file.

5. Run the PostgreSQL `pg_dump` command on the database to backup the database and output this to a file in an sql format.

```
[-bash-4.1$] ./pg_dump <db_name> > <location_of_dump_file>
```

Example

```
[-bash-4.1$] ./pg_dump wfsdb > /var/tmp/wfsdb_11_Oct_2015_12_22.sql
```

6. Run the `pg_dumpall` command to create a backup of all databases.

```
[-bash-4.1$] ./pg_dumpall > <location_of_dump_file>
```

Example

```
[-bash-4.1$] ./pg_dumpall > /var/tmp/postgres_alldb_11_Oct_2015_12_31.sql
```

The backup file is now available at the the directory provided to the `pg_dump/pg_dumpall` script.

Option 5 of the `postgres_admin` script available at `/opt/ericsson/pqsql/util/postgres_admin.sh` can be used to display a list of all databases and the current used space for each.

Note: Database backup files stored in `/var/tmp` should only temporarily exist due to disk space and security considerations. These files should be removed when they are no longer needed.

Results

The required PostgreSQL database backups are taken.

7.17.8 PostgreSQL Database Space Maintenance Options

This Utility frees up unused PostgreSQL database space.

Note: This is regarded as an **EMERGENCY OPERATION**

Background

Where an ENM deployment runs out of PostgreSQL volume space, an option to recover space is to release the space occupied by unused rows/tuples - also referred to in PostgreSQL as tuple bloat.

To avoid the PostgreSQL volume space filling up, which could cause an ENM outage, this utility removes the tuple bloat that the default PostgreSQL Vacuum process has not re-allocated.

The system should have a recent backup and you may take an optional backup of the database that the tuple bloat is being removed from. This option is provided for in the utility.

Connectivity to the database that the utility is working on will be lost while recovery is taking place. This loss of connectivity can last between 2 or 3 minutes per GB of DB Size, depending on such factors as bloat level, table size, row length, or row contents.

Once the Vacuum completes, indexes are recreated and connectivity resumes. If the process is killed, connectivity automatically resumes.

It is advisable to not interrupt the process, and in such a scenario rerun the process on the affected DB as soon as possible following the interruption.

If the free space available on the file system is less than the size of the largest database tables, use the utility on smaller databases to free up enough space to accommodate the larger databases.

This procedure is executed on the largest databases, starting with the 3rd largest, and then progressing through the 2nd largest, then the largest, presuming total free space is greater than the size of the largest DB.

The procedure should be run when no elective procedures are running. It should not be run during backup and ENM Upgrade activities.

Prerequisites

— Knowledge about ENM system admin.

— Access to the host where postgres is running.

— An ENM backup has been taken before the starting this procedure.

— Free space on the file system greater than the size of the largest database.

— Not be run during backup and ENM Upgrade activities.

Running the Utility

1. Log in to the active database server and switch user to root, then execute the utility to validate space used by PostgreSQL:

```
#/opt/ericsson/pgsql/util/postgres_admin.sh -M
```

A report is presented showing DB Usage. Overall usage should exceed 50% before running the Vacuum Utility.

2. Execute the utility where PostgreSQL is running as user root;

```
#python /opt/ericsson/pgsql/util/pg_maintenance_vacuum.py
```

```
## Before proceeding, it is advisable to have a valid OMBS backup.
## This is an intrusive operations and should only be executed during a quie → t time, ideally a maintenance window.
## Connections to the Database under processing will be limited during this → process.
Do you wish to proceed (y/n)
```

Choose y

3.
```
Select an action to proceed with
1) Display Database Information
2) Create Database Backup
3) Vacuum Database
0) Exit
```

Choose 1

4.
```
Display Database Information;
Generates a Usage Report..
Sample
Generating usage report for all Databases..
No.       DB Name             DB Space ------------------------------------ → ---
1         kpiservdb           14 GB
2         importdb            2251 MB
3         flsdb               639 MB
4         exportds            212 MB
....
Select DB to continue or '0' to Exit :
```

In this example we use `importdb` database , so manually type in keyboard "2" as this corresponds with the `importdb` database.

Note: Running Vacuum should only be done on application databases. Internal PostgreSQL databases such as template0, template1, and postgres databases should not be considered vacuum candidates.

```
importdb DB selected for processing

 >> Filesystem Size info for the DB importdb Database name : importdb Databa →
se directory : /ericsson/postgres/data/base/19989

Database OID : 19989

importdb database space used : 2251 MB

Postgres space used : 20G

Total Postgres Space : 110G

Percentage space used : 19%

Available Space: 86G

>> Largest tables from importdb database

(max 5):

import_operation        | 1596 MB

import_simple_attribute | 535 MB  job

..............

> Tuple information for the Table: job  table_len | tuple_count | tuple_len  →
| tuple_percent | dead_tuple_count | dead_tuple_len | dead_tuple_percent | f →
ree_space | free_percent -----------+-------------+-----------+------------ →
--+------------------+----------------+--------------------+------------+--- →
-----------   49848320 |       34158 |  44070818 |         88.41 |            →
    436 |         568434 |               1.14 |    4767844 |         9.56 (1 →
 row)

> Tuple information for the Table: operation  table_len | tuple_count | tupl →
e_len | tuple_percent | dead_tuple_count | dead_tuple_len | dead_tuple_perce →
nt | free_space | free_percent -----------+-------------+-----------+------- →
--------+------------------+----------------+--------------------+---------- →
--+--------------   20520960 |      134851 |  19264367 |         93.88 |      →
          0 |              0 |                  0 |     505608 |         2 →
.46 (1 row)

.........
Do you wish to return to main menu (y/n)
```

Create Database Backup

```
Select an action to proceed with

1) Display Database Information

2) Create Database Backup

3) Vacuum Database

0) Exit

Select an option
```

Choose 2

```
Take a DB Backup:

<DB List Provided>

Select DB to continue or '0' to Exit :
```

For the purpose of this example we have chosen database `importdb`, option 2

```
importdb DB selected for processing

Enter path to store DB backup (default /ericsson/enm/dumps) <enter default>

Available Space: <<available space in path provided>> | Database size: <<size of  →
 databases selected>>

>> Creating backup for the database importdb at

>> /ericsson/enm/dumps/pg_dump_importdb_28-02-2019-15-38.tar

Backup of database postgres at /ericsson/enm/dumps/pg_dump_postgres_01-03-2019-1  →
5-59.tar completed
Do you wish to return to main menu (y/n)
```

Choose y

Run the Vacuum on your selected Database

```
Vacuum Database

Select DB to continue or '0' to Exit :
```

Choose 2

```
importdb DB selected for processing

NOTE : The following steps will restrict access to the DB

Do you wish to proceed (y/n)
```

Choose y

```


>> Restricting access to Database importdb. This may take a few minutes

Tuple Information before Vacuuming: >

Tuple information for the Table: import_operation

         table_len     | tuple_count | tuple_len           | tuple_percent  | de  →
ad_tuple_count  | dead_tuple_len | dead_tuple_percent | free_space | free_percen  →
t

-----1462714368 |  4404803   | 1328039808           |         90.79        |      →
        3531              |         1071776      |               0.07             →
     |   95099836 |       6.5 (1 row)

...

 >> Updating stat for the DB importdb may take 1 min per GB  >> Running full vac  →
uum for the DB importdb allow up to 3 mins per GB  >> Reindexing the DB importdb  →
 - may take several minutes


Generating usage report for all Databases..
```

```
Info
                                                Before Vacuuming      After Vac →
uuming
=====================================================================
Database space used                  2251 MB                     2158 MB
Total Space Reclaimed         -                                          88.7M
Current Postgres Space Used             20G                          20G
Total Postgres Database Space        110G                           110G
Total Available Space                             85G                          85G
>> Restoring access to Database importdb.
>> Access Restored to importdb.
Total Time for Vacuum Procedure on importdb database:: 0:01:39.770844 Do you wis →
h to return to main menu (y/n)
```

Choose `y`

```
Select an action to proceed with
1) Display Database Information
2) Create Database Backup
3) Vacuum Database
0) Exit
Select an option :
```

Choose `0`

```
Exiting !!
```

Note: The entire operation is logged under `/var/log/messages` with the TAG < pg_maintenance_vacuum: >

Running `vacuumdb` is not guaranteed to free up space as on some databases there may be no dead tuples or tuple bloat.

Remove the Database Backup

If you are satisfied the space is recovered, the application is working as expected, and a back-up of the database was created during this operation, delete the saved PostgreSQL database backup.

```
rm /ericsson/enm/dumps/pg_dump_importdb_28-02-2019-15-38.tar
```

7.17.9 PostgreSQL File System Monitor

Option 15 from `/opt/ericsson/pqsql/util/postgres_admin.sh` provides information about PostgreSQL file system, databases, and its largest tables.

Utility also generates a report with databases that exceed allocated storage resources and are candidates for PostgreSQL vacuuming.

Note: The information below is for is for demonstration purposes and may not correspond to actual production data.

```
*****************************************************************
PostgreSQL File System Monitor
*****************************************************************



-------------------------
Postgres Mount Information
-------------------------
+------------+------------------+-----------------+----------------------+------  →
-----------+
| Mount Name | Total Space (GB) | Used Space (GB) | Available Space (GB) | Perce  →
ntage Used |
+------------+------------------+-----------------+----------------------+------  →
-----------+
| postgres   | 110.00           | 41.00           | 66.00                | 39%    →
           |
+------------+------------------+-----------------+----------------------+------  →
-----------+


----------------------------------
Current Database Sizes Vs Allocated
----------------------------------
+------------------+---------+-------------------+---------------------+-------  →
---------------------+-------------------------+--------------------------+
| Database Name     | ID      | Current Size (MB) | Allocated Size (MB) | Larges  →
t Table Name          | Current Table Size (MB) | Allocated Table Size (MB) |
+------------------+---------+-------------------+---------------------+-------  →
---------------------+-------------------------+--------------------------+
| kpiservdb         | 20831   | 21295.75          | 32768.00            | kpi_da  →
ta                    | 16486.88                | 31744.00                 |
| flsdb             | 20781   | 11008.51          | 18432.00            | pm_rop  →
_info                 | 10970.73                | 11264.00                 |
| importdb          | 19989   | 4898.98           | 11264.00            | import  →
_operation            | 3496.10                 | 6144.00                  |
| flowautomationdb  | 16393   | 707.69            | 512.00              | act_ge  →
_bytearray            | 255.99                  | 256.00                   |
| wfsdb_shmcoreserv | 19200   | 457.70            | 2560.00             | act_ru  →
_variable             | 257.17                  | 1024.00                  |
| exportds          | 16394   | 310.65            | 1512.00             | partit  →
ion_execution         | 119.91                  | 756.00                   |
| wfsdb_secserv     | 19991   | 253.99            | 2048.00             | act_ru  →
_meter_log            | 219.10                  | 1024.00                  |
| wfsdb_apserv      | 18412   | 128.70            | 200.00              | act_ru  →
_meter_log            | 108.95                  | 160.00                   |
| pkimanagerdb      | 17433   | 71.28             | 4608.00             | certif  →
icate_generation_info | 20.83                   | 2048.00                  |
| pkicoredb         | 16587   | 57.15             | 4608.00             | certif  →
icate                 | 16.48                   | 2048.00                  |
| idenmgmt          | 20830   | 48.18             | 2048.00             | ldap_p  →
osix_group            | 9.07                    | 1536.00                  |
| sfwkdb            | 16467   | 28.62             | 128.00              | eservi  →
ce_info               | 10.65                   | 64.00                    |
| configds          | 17315   | 20.24             | 150.00              | partit  →
ion_execution         | 8.99                    | 64.00                    |
| pkiratdpsdb       | 17404   | 10.30             | 400.00              | tdpsda  →
ta                    | 4.44                    | 320.00                   |
| kapsdb            | 17243   | 7.26              | 128.00              | keypai  →
r_info                | 0.08                    | 96.00                    |
| admindb           | 6742478 | 7.08              | 1024.00             | db_ver  →
sion                  | 0.05                    | 128.00                   |
| jberetdb          | 19990   | 7.04              | 64.00               | config  →
uration               | 0.08                    | 32.00                    |
| pkicdpsdb         | 16557   | 6.94              | 400.00              | cdps_c  →
rl                    | 0.09                    | 320.00                   |
| itservicesdb      | 19988   | 6.92              | 64.00               | contro  →
l                     | 0.04                    | 32.00                    |
| pkirascepdb       | 16530   | 6.91              | 400.00              | db_ver  →
```

```
sion                  | 0.08                    | 320.00                    |
| pkiracmpdb        | 17374   | 6.88              | 400.00               | db_ver →
sion                  | 0.08                    | 320.00                    |
| domainproxydb     | 17373   | 6.88              | 64.00                | versio →
n                     | 0.05                    | 32.00                     |
| bulknodecli       | 2812248 | 6.77              | 20.00                | bulkno →
decli_job             | 0.02                    | 18.00                     |
| ebsm              | 17432   | 6.70              | 1512.00              | No tab →
les                   | -1.00                   | 512.00                    |
+-------------------+---------+-------------------+----------------------+------- →
----------------------+-------------------------+---------------------------+


---------------------------
Exceeds Allocated Resources
---------------------------
+------------------+-------+-------------------+--------------------+---------- →
----------+-------------------------+---------------------------+
| Database Name    | ID    | Current Size (MB) | Allocated Size (MB) | Largest T →
able Name | Current Table Size (MB) | Allocated Table Size (MB) |
+------------------+-------+-------------------+--------------------+---------- →
----------+-------------------------+---------------------------+
| flowautomationdb | 16393 | 707.69            | 512.00              | act_ge_by →
tearray   | 255.99                  | 256.00                    |
+------------------+-------+-------------------+--------------------+---------- →
----------+-------------------------+---------------------------+
```

7.17.10 Remove Expiry Period via Optional Argument

Instead of using the PostgreSQL DBA Utility interactive menu, the script can be executed by passing the optional argument -E. The -E optional argument will remove the Postgres Role's expiry period, setting the expiration period to infinity.

```
[root@<DB-node> ~]# /opt/ericsson/pgsql/util/postgres_admin.sh -E
```

Sample Output:

```
================================================================================
                        Remove Postgres Role's Expiry
================================================================================

postgres_pass_expiry: [INFO]: Attempting to remove Postgres role's validity peri →
od.
postgres_pass_expiry: [INFO]: Successfully removed Postgres role's validity peri →
od.

To add a validation period for the Postgres role refer to ENM System Admin Guide →
 -1/1543-AOM 901 151
```

Reference List

[1] *OSS RC 14B Client Installation Instructions document update for ENM*, *21/1531-APR 901 0127*

Section: 8 Setting up AMOS and EM Application in OSS-RC

[2] *Citrix Presentation Server for UNIX Administrator's Guide*

Chapter 5: Publishing Applications and Desktops

[3] *ENM Security System Administrator Guide*,2/1543-aom9010151 Uen

[4] *ENM Identity and Access Management System Administrator Guide*, 2/1543-aom9010151-1 Uen

[5] *ENM Network Security Configuration System Administrator Guide*2/1543-aom9010151-2 Uen

[6] *ENM Public Key Infrastructure System Administrator Guide*2/1543-aom9010151-3 Uen

[7] *User Administration (CLI)*, 112/19080-cra2500056/1 Uen

[8] *Operator Access Handling*, 22/1543-axb25017 Uen

[9] *Configuring IP-Based Interfaces*, 36/1543-axb25017 Uen

[10] *ENM Product Description*, 1/1551-AOM 901 151

[11] *AMOS, Advanced MO Scripting, User Guide*, 6/1553-apr9010253 Uen

[12] *ENM Installation Instructions*, (Available from local Ericsson Support)

[13] *FLARE and Firmware Handling guide for HP/EMC*, (Available from local Ericsson Support)

[14] *ENM Site Engineering Document*, (Available from local Ericsson Support)

[15] *ENM Backup and Restore System Administrator Guide*, 3/1543-AOM 901 151

[16] *ENM Library Typographic Conventions*, 10/1551-AOM 901131

[17] *OSS Configuration for ENIQ Statistics*, (Available from Ericsson Network IQ Statistics CPI Library)

[18] *ENM Upgrade Instructions*, (Available from local Ericsson Support)

[19] *ENM Troubleshooting Guide*, 1/15901-AOM 901 151

[20] *ENM System Administrator Guide*, 1/1543-AOM 901 151

[21] *ENM Configuration System Administrator Guide*, 1/1543-AOM 901 151-1

[22] *ENM Monitoring System Administrator Guide*, 1/1543-AOM 901 151-2

[23] *ENM Performance Management System Administrator Guide*, 1/1543-AOM 901 151-3

[24] *Performance Management Description*, 3/1551-hsc10550/1 Uen

[25] *Manage Performance User Guide*, 14/1553-lza7016014/1 Uen

[26] *UE Tracer Technical Product Description*, 54/22102-axb25005/8-v2

[27] *EPG System Administrator Guide*, 30/1543-cra 119 2158-v1 Uen

[28] *Dynamic CM Import/Export Interwork Description*, 3/15519-CNA 403 2977

[29] *ENM Parameter List*, 1/190 59-AOM 901 151
[30] *ENM Node Hardening Guidelines and Instructions*, 1/174 73-AOM 901 151
[31] *ENM System Monitor User Guide*, 1/1553-CNA 403 3115
[32] *Installing Core Network Operations Manager*, Available from CNOM CPI EN/LZN 704 0220
[33] *Small Integrated ENM System Administration Guide*, 1/1543 CAN 403 3456
[34] *ENM on Cloud Backup and Restore System Administrator Guide*, 5/1543-AOM 901151
[35] *ENM Operators Guide*, 1/1553-AOM 901 151
[36] *ENM Privacy User Guide*, 2/1553-AOM 901 151
[37] *Installing UDC Dashboard*, Available from UDC Dashboard CPI EN/LZN 702 0489, available from local Ericsson support
[38] *VNF Lifecycle Management Upgrade Instructions* 1/153 72-CNA 403 331
[39] *ENM on Cloud Upgrade Instructions* 2/153 72-AOM 901 151
[40] *ENM Configuration Troubleshooting Guide*, 1/159 01-AOM 901 151-1
[41] *Flexible PM Statistics User Guide* 1/1553-HSD 101 02/1
[42] *SNMP User Guide MINI-LINK 6352* 8/1553-HRA 901 17/7