ERICSSON

ENM Troubleshooting Guide

Check List

1/159 01-AOM 901 151 Uen DY

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

Contents

1 About the ENM Troubleshooting Guide

The tasks contained in the Troubleshooting Guide are not intended to be part of routine maintenance and operational procedures. The troubleshooting tasks respond to specific scenarios or event that can occur in the system.

ENM Troubleshooting Guide is referenced in the event of system fail-over or other scenarios that can result in abnormal status.

This document provides the following information:

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

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

— ENM Configuration Troubleshooting Guide

— ENM Monitoring Troubleshooting Guide

— ENM Performance Troubleshooting Guide

— ENM Security Troubleshooting Guide

Target Groups

— 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 Troubleshooting Tasks for the Platform in LITP Based Deployments

This section describe the tasks for the platform in LITP based deployments.

5.1 Hostname Change Breaks PuppetDB and MCollective

If you inadvertently change the hostname of the LMS to that of another server after you have installed LITP, the Puppet certificates may become corrupted. This may occur even if you have attempted to revert the hostname to original name of the LMS.

To resolve this issue, perform the following actions as the root user:

Steps

1. Reset the hostname of the LMS to the correct value (one it was installed with).
2. Restart the Puppet Server service by entering the following command:

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

3. Restart the Puppet service by entering the following command:

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

4. Restart the MCollective service by entering the following command:

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

5. Restart the PuppetDB service by entering the following command:

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

6. Restart the RabbitMQ server:

```
[root@ms1 ~]# service rabbitmq-server restart
```

7. Check the Puppet status to verify that Puppet has finished processing and the hostname change has completed successfully:

```
[root@ms1 ~]# mco puppet status
* [ ============================================================> ] 5 / 5

     ms1: Currently idling; last completed run 1 minutes 10 seconds ago
```

```
    node1: Currently idling; last completed run 29 seconds ago
    node3: Currently idling; last completed run 1 minutes 00 seconds ago
    node4: Currently idling; last completed run 10 seconds ago
    node2: Currently idling; last completed run 1 minutes 00 seconds ago
...
Finished processing 5 / 5 hosts in 20.16 ms
```

Results

The hostname is correct, and the Puppet, MCollective, PuppetDB, and RabbitMQ services are restored and operating normally.

5.2 Purge PuppetDB When /var Exceeds Maximum Capacity

Perform this procedure if PuppetDB database is corrupted because the `/var` partition is full. Complete the following tasks on the MS as the `root` user.

Note: The following commands are only applicable if `/var` partition becomes full outside the running of a LITP plan. If the `/var` partition becomes full, PuppetDB is only one application that may become faulty. This procedure assumes that only PuppetDB is faulty and does not consider other possible failures that can happen when there is insufficient space for an application to write to `/var`. Even if the procedure described below is successful other failure scenarios may cause corruptions that will only become apparent during a later LITP operation.

Prerequisites

An error message similar to the following is seen in `/var/log/puppetdb/puppetdb.log`.

```
2016-10-24 02:33:56,659 ERROR [ConcurrentQueueStoreAndDispatch] [kahadb.MessageD →
atabase] KahaDB failed to store to Journal
java.io.IOException: No space left on device
        at java.io.RandomAccessFile.writeBytes0(Native Method)
        at java.io.RandomAccessFile.writeBytes(RandomAccessFile.java:520)
        at java.io.RandomAccessFile.write(RandomAccessFile.java:550)
        at org.apache.kahadb.journal.DataFileAppender.processQueue(DataFileAppen →
der.java:359)
        at org.apache.kahadb.journal.DataFileAppender$1.run(DataFileAppender.jav →
a:188)
2016-10-24 02:33:56,664 ERROR [ActiveMQ Task-7549] [kahadb.MessageDatabase] Kaha →
DB failed to store to Journal
java.io.IOException: No space left on device
        at java.io.RandomAccessFile.writeBytes0(Native Method)
        at java.io.RandomAccessFile.writeBytes(RandomAccessFile.java:520)
        at java.io.RandomAccessFile.write(RandomAccessFile.java:550)
        at org.apache.kahadb.journal.DataFileAppender.processQueue(DataFileAppen →
der.java:359)
        at org.apache.kahadb.journal.DataFileAppender$1.run(DataFileAppender.jav →
a:188)
2016-10-24 02:33:56,665 WARN  [ActiveMQ Task-7549] [transaction.LocalTransaction →
] Store COMMIT FAILED:
java.io.IOException: No space left on device
```

Follow this process to clean and recreate the database which may resolve the issue.

Note: If this procedure fails, the only option remaining is to restore the management server. For more information, refer to the ENM Backup and Restore System Administration Guide.

Steps

1. Cleanup the `/var` partition.

   Move any files you have stored in `/var/tmp` and any of its sub directories to `/software`.

2. Determine if the yum database has been corrupted on the ENM MS by completing the steps described in the Verify the Integrity of the ENM MS RPM Database topic of the ENM Installation Instructions.

3. Disable the puppet agent:

   ```
   [root@ms-1 ~]# puppet agent --disable
   ```

4. Verify that the puppet agent is disabled. In the example below the hostname of the MS is ms-1:

   ```
   [root@ms-1 var]# mco puppet status -I ms-1
   * [ ============================================================> ] 1 / 1

      ms-1: Currently disabled; last completed run 7 minutes 46 seconds ago

   Summary of Applying:

      false = 1

   Summary of Daemon Running:

      running = 1

   Summary of Enabled:

      disabled = 1

   Summary of Idling:

      true = 1

   Summary of Status:

      disabled = 1

   Finished processing 1 / 1 hosts in 18.02 ms
   [root@ms-1 var]#
   ```

   a. Restart RabbitMQ server if an error message similar to the following is displayed.

      ```
      The puppet application failed to run, use -v for full error backtra
      ce details: Could not connect to RabbitMQ Server: Stomp::Error::Max
      ReconnectAttempts
      [root@ms-1 var]# service rabbitmq-server restart
      ```

   b. Check the status of service.

```
[root@ms-1 rabbitmq]# service rabbitmq-server status
```

If output similar to the following is displayed, continue to *step c*.

```
[root@ms-1 rabbitmq]# service rabbitmq-server status
Status of node rabbit@lms-1 ...
Error: unable to connect to node rabbit@lms-1: nodedown

DIAGNOSTICS
===========

attempted to contact: [rabbit@ms-1]

rabbit@lms-1:
  * connected to epmd (port 4369) on lms-1
  * epmd reports: node 'rabbit' not running at all
                  no other nodes on lms-1
  * suggestion: start the node

current node details:
- node name: 'rabbitmq-cli-12089@lms-1'
- home dir: /var/lib/rabbitmq
- cookie hash: 3d4JzsoKgcZP05A3yqsqTw==
```

c. Execute the following commands to resolve RabbitMQ issue.

```
[root@ms-1 rabbitmq]# mv /var/lib/rabbitmq/mnesia/rabbit\@lms-1/recovery.dets →
 /var/tmp/
You have mail in /var/spool/mail/root

[root@ms-1 rabbitmq]# service rabbitmq-server stop

Stopping rabbitmq-server: RabbitMQ is not running
rabbitmq-server.

[root@ms-1 rabbitmq]# service rabbitmq-server start

Starting rabbitmq-server: SUCCESS
rabbitmq-server.

[root@ms-1 rabbitmq]# service rabbitmq-server status

Status of node rabbit@lms-1 ...
[{pid,54134},
 {running_applications,
     [{rabbitmq_management,"RabbitMQ Management Console","3.5.4"},
      {rabbitmq_web_dispatch,"RabbitMQ Web Dispatcher","3.5.4"},
      {webmachine,"webmachine","1.10.3-rmq3.5.4-gite9359c7"},
      {mochiweb,"MochiMedia Web Server","2.7.0-rmq3.5.4-git680dba8"},
```

Output similar to the following indicates that RabbitMQ issues are resolved.

```
[root@ms-1 rabbitmq]# service rabbitmq-server status
Status of node rabbit@lms-1 ...
[{pid,54134},
 {running_applications,
     [{rabbitmq_management,"RabbitMQ Management Console","3.5.4"},
      {rabbitmq_web_dispatch,"RabbitMQ Web Dispatcher","3.5.4"},
      {webmachine,"webmachine","1.10.3-rmq3.5.4-gite9359c7"},
      {mochiweb,"MochiMedia Web Server","2.7.0-rmq3.5.4-git680dba8"},
```

5. Stop the PuppetDB service:

```
[root@ms1 ~]# service puppetdb stop
Stopping puppetdb:         [  OK  ]
```

6. Purge the database:

```
[root@ms1 ~]# sudo -u postgres dropdb puppetdb
```

7. Delete puppetdb files under `/var/lib/puppetdb/mq/localhost/KahaDB/`:

```
[root@ms1 ~]# rm /var/lib/puppetdb/mq/localhost/KahaDB/*
```

8. Restart Puppet Server on the MS:

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

9. Enable the puppet agent:

```
[root@ms-1 ~]# puppet agent --enable
```

10. Verify that the puppet agent is enabled. In the example below the hostname of the MS is ms-1:

```
[root@ms-1 var]# mco puppet status -I ms-1
 * [ ============================================================> ] 1 / 1
   ms-1: Currently idling; last completed run 12 minutes 33 seconds ago
Summary of Applying:
   false = 1
Summary of Daemon Running:
   running = 1
Summary of Enabled:
   enabled = 1
Summary of Idling:
   true = 1
Summary of Status:
   idling = 1

Finished processing 1 / 1 hosts in 8.27 ms
```

11. Run Puppet to recreate the database; wait until Puppet has finished applying the catalogs. In the example below the hostname of the MS is `ms1`:

```
[root@ms1 ~]# mco puppet runonce -I ms1
* [ ============================================================> ] 1 / 1
Finished processing 1 / 1 hosts in 5083.69 ms
```

Wait until Puppet has finished applying the catalogs. You may receive `failed to connect to puppetdb` messages during the time that these changes are being applied.

If you receive a `Puppet is currently applying a catalog, cannot run now failed to connect to puppetdb` message, rerun the command above.

Once the Puppet run has finished, a message similar to the following is visible in the `/var/log/messages` log file:

```
Apr 23 14:40:45 cloud-ms-1 puppet-agent[21442]: (/Stage[main]/Puppetdb::Data →
base::Postgresql/Postgresql_litp::Server::Db[puppetdb]/Postgresql_litp::Serv →
er::Database_grant[GRANT puppetdb - all - puppetdb]/Postgresql_litp::Server: →
:Grant[database:GRANT puppetdb - all - puppetdb]/Postgresql_psql[GRANT ALL O →
N DATABASE "puppetdb" TO "puppetdb"]/command) command changed 'notrun' to 'G →
RANT ALL ON DATABASE "puppetdb" TO "puppetdb"'
..
..
..
..
Apr 23 14:41:47 cloud-ms-1 puppet-agent[21442]: Finished catalog run in 98.9 →
9 seconds
```

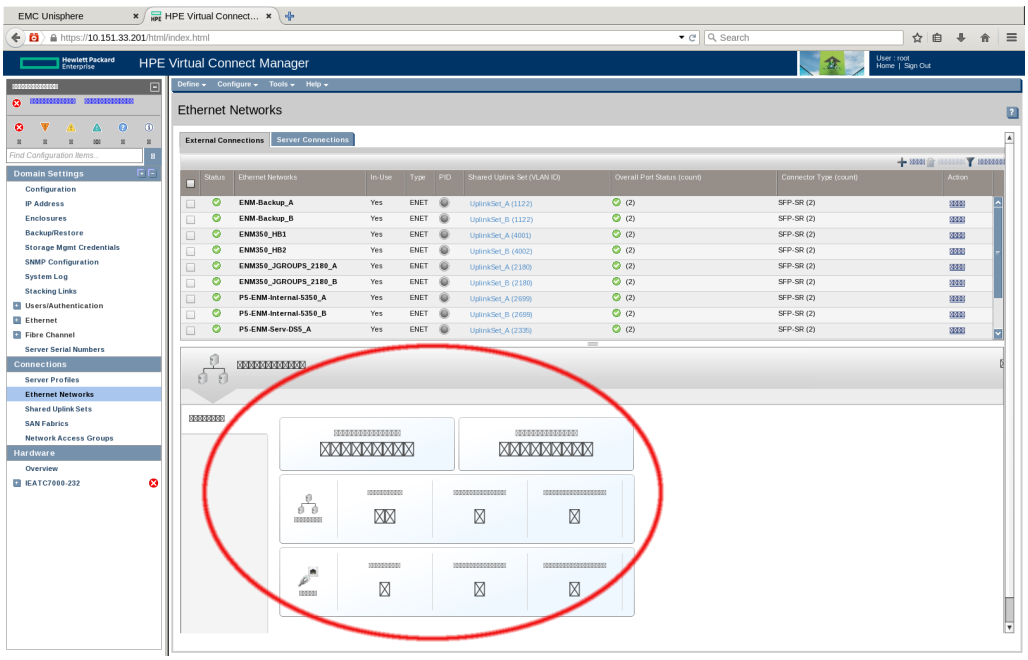
A successful Puppet run indicates that the PuppetDB database and service are operational.

Results

PuppetDB database and service are restored and operating normally.

5.3 Missing Font or Character Boxes When Accessing Management GUI Remotely

When accessing a management GUI remotely through the Management Server (MS), user may see missing font or character boxes as illustrated in the following example:



Prerequisites

You have completed the steps in the *Launch Firefox Remotely* from the *Management Server* section of the ENM System Administrators Guide.

Steps

1. As the `root` user on the MS, check if the fonts package is installed by entering the following command:

   ```
   $ sudo yum list all | grep dejavu-sans-fonts
   ```

2. If `dejavu-sans-fonts` is returned, then the font package is installed and no further action is necessary. If `dejavu-sans-fonts` is not returned, enter the following command to install the font package:

   ```
   $ sudo yum install -y grep dejavu-sans-fonts

   dejavu-sans-fonts.noarch                2.33-6.el7                  @anac
   onda
   bpg-dejavu-sans-fonts.noarch            2.28-3.el7                  base

   php-tcpdf-dejavu-sans-fonts.noarch      6.2.13-1.el7                epel
   ```

3. Repeat step 1 to check that the package is installed.

Results

The fonts package successfully installs.

5.4 Accessing Java Based GUIs and Flash Plugins based GUIs using Firefox

The following GUIs are no longer supported in Firefox.

— Java based GUIs in versions later than Firefox 52 Extended Support Release (ESR).

— Flash plug-ins based GUI in versions later than Firefox 68 ESR.

With the recent version of Firefox, the following error messages are prompted:

— `JRE is required for this application to run` when trying to access a Java based Management GUI (for instance, the EMC Unisphere GUI).

— `The Adobe Flash plugin has crashed` when trying to access a Flash plug-in based GUI (for instance, the HP Virtual Connect Manager GUI).

If a Java based Management GUI or Flash plug-ins based GUI have to be accessed using the Firefox browser on the Management Server, temporarily downgrade the Firefox browser to Firefox 52 version. You may also need to configure the **Exception Site List** in the **Java Control Panel**.

All alternative ways to access the Java based Management GUI and flash plug-ins based GUI must be considered before using the following procedure (for instance, using an alternative browser from an alternative location).

Prerequisites

None.

Steps

1. Downgrade to Firefox 52, as the `root` user, from the ENM MS:

   ```
   [root@ms-1 ~]# yum downgrade -y /var/www/html/6/os/x86_64/Packages/firefox-52.8.0-1.el6_9.x86_64.rpm
   ```

2. Launch the Firefox browser by completing the steps in the *Launch Firefox Remotely from the Management Server* section of the ENM System Administrator Guide.

3. Enter the IP address of the Management GUI in the URL address bar of the browser.

   — If you receive a message, `Application Blocked by Java Security`:

   a. Launch the **Java Control Panel**, as the `root` user, from the ENM MS.

   ```
   [root@ms-1 ~]# /usr/java/<jre_version>/bin/ControlPanel
   ```

b. Select the **Security** tab and click **Edit Site List**.

c. Click **Add** in the **Exception Site List** window, enter the IP address of the Management GUI, then click **OK**.

d. If you receive a security warning about including HTTP locations displays, click **Continue** to accept the location.

— If you receive security warnings when starting the Management GUI, select **I accept the risk and want to run this application**, then click **Run**.

— If any certificate warnings appear, click **Accept for Session**.

4. Once the browsing session is complete on the Management GUI, close all the Firefox browser windows and reinstall the latest secure version of Firefox, as **root** user from the ENM MS.

```
[root@ms-1 ~]# yum update -y firefox
```

5.5 Performance Issue When Accessing EMC Unisphere GUI Remotely

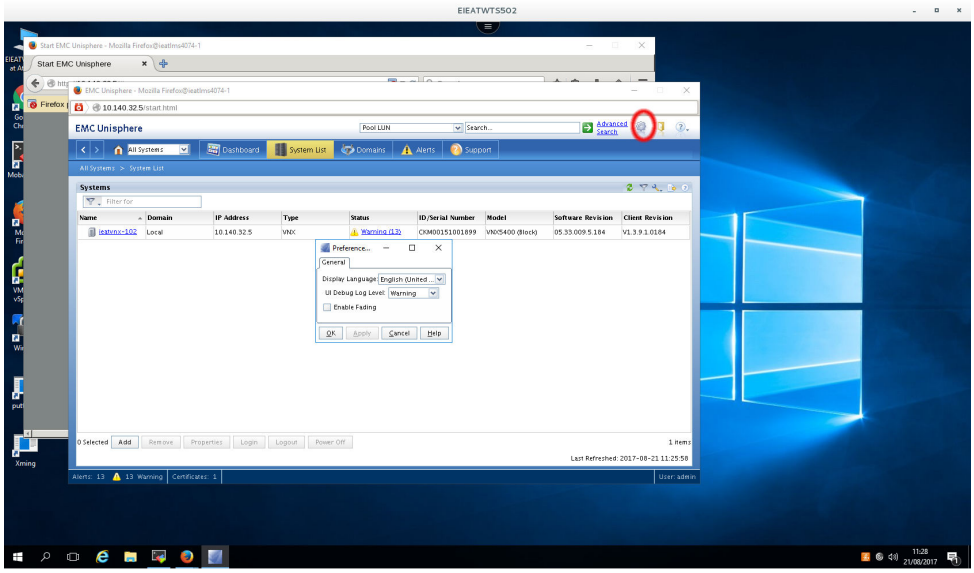
Performance issues can occur when accessing the EMC Unisphere remotely through Mozilla Firefox on the Management Server. This is caused by the fading effect of Unisphere, which slows down the loading time for the interface.

Prerequisites

Complete the procedure *Launch Firefox Remotely* mentioned in the ENM System Administrator Guide.

Steps

1. Click the **Settings** icon on the top right side of the interface.
2. Clear the **Enable Fading** check box in the Preferences dialog box.
3. Click **Apply** and then click **OK**.



Results

The performance of ENM Unisphere improves.

5.6 VCS Service Group Failure

If the `enm_healthcheck.sh` script fails with a `There appears to be a fault with the one or more VCS Service Groups` error, use this procedure to resolve the error.

Steps

1. Run the `enm_healthcheck.sh` script in verbose mode to view the VCS Service Groups that are `FAULTED` or not `ONLINE` as expected:

   Note: If the `GroupState` property is set to `OK` for a VCS Service Group, then it is okay for that VCS Service Group to be `OFFLINE`.

   ```
   # /opt/ericsson/enminst/bin/enm_healthcheck.sh --verbose
   ```

   For example:

```
[root@ieatlms7522 bin]# ./enm_healthcheck.sh --action node_fs_healthcheck
Beginning ENM pre-Healthchecks
Node Status: PASSED
Completed ENM pre-Healthchecks
Checking if peer node filesystems do not exceed
90% for NAS
92% for versnt-neo4j, elasticsearch
80% for all other filesystems

Obtaining NAS information from the LITP model
Successfully Completed Node Filesystem Healthcheck
```

```
[root@ieatlms7522 bin]# /opt/ericsson/enminst/bin/enm_healthcheck.sh --verbose
Beginning ENM pre-Healthchecks
  ------------  ------
        System   State
  ------------  ------
   ieatlms7522  ONLINE
  ieatrcxb3388  ONLINE
  ieatrcxb3133  ONLINE
  ieatrcxb3529  ONLINE
  ieatrcxb3134  ONLINE
  ieatrcxb3300  ONLINE
  ieatrcxb3301  ONLINE
  ieatrcxb3565  ONLINE
  ieatrcxb3566  ONLINE
  ------------  ------
Node Status: PASSED
Completed ENM pre-Healthchecks
Beginning ENM System Healthcheck
----------------------------------------------------------------
CHECKING VM RAM AND CPU USAGE PER NODE
----------------------------------------------------------------
Exporting model ...
Gathering VM RAM and CPU resources from each node
Checking model hardware resources against actual hardware resources on svc-1
Checking model hardware resources against actual hardware resources on svc-2
Checking model hardware resources against actual hardware resources on svc-3
Checking model hardware resources against actual hardware resources on svc-4
  -----------  -----  ---------  ----------------------  -------------  ------------------  ----  →
-
      Cluster   Node  CPUs used  CPU over-provision ratio  RAM used (MB)  RAM available (MB)  Stat  →
e
  -----------  -----  ---------  ----------------------  -------------  ------------------  ----  →
-
  svc_cluster  svc-3         88                     2.8         193536               64757     0  →
K
  svc_cluster  svc-4         88                     2.8         193536               64757     0  →
K
  svc_cluster  svc-1         94                     2.9         198656               59637     0  →
K
  svc_cluster  svc-2         94                     2.9         198656               59637     0  →
K
  -----------  -----  ---------  ----------------------  -------------  ------------------  ----  →
-
Successfully Completed Hardware Resources Healthcheck
----------------------------------------------------------------
CHECKING ALL NODES FOR STALE MOUNTS
----------------------------------------------------------------
Checking all nodes for stale mounts

Successfully Completed Stale Mounts Healthcheck
ENM STALE MOUNT HEALTHCHECK: PASSED
----------------------------------------------------------------
CHECKING MS, NAS AND PEER NODE FILESYSTEM USAGE
----------------------------------------------------------------
Checking if peer node filesystems do not exceed
90% for NAS
92% for versnt-neo4j, elasticsearch
80% for all other filesystems

Obtaining NAS information from the LITP model
  -------------------------------  ----
             ieatlms7522
  -------------------------------  ----
                       FileSystem  Use%
  -------------------------------  ----
      /dev/mapper/vg_root-lv_root   26%
                             tmpfs    1%
                         /dev/sda1   17%
      /dev/mapper/vg_root-lv_home    1%
  /dev/mapper/vg_root-lv_software   43%
       /dev/mapper/vg_root-lv_var    6%
   /dev/mapper/vg_root-lv_var_log    2%
   /dev/mapper/vg_root-lv_var_www   36%
   /dev/mapper/vg_root-vg1_fs_vms   22%
  -------------------------------  ----
  ------------------------------------  ----
                     sfs
  ------------------------------------  ----
                             FileSystem  Use%
  ------------------------------------  ----
```

```
         /dev/vx/dsk/sfsdg/ENM665-cnom    5%
         /dev/vx/dsk/sfsdg/ENM665-pmul    5%
         /dev/vx/dsk/sfsdg/ENM665-alex    5%
      /dev/vx/dsk/sfsdg/ENM665-hcdumps   18%
   /dev/vx/dsk/sfsdg/ENM665-solrautoid    5%
   /dev/vx/dsk/sfsdg/ENM665-config_mgt    3%
         /dev/vx/dsk/sfsdg/ENM665-solr    3%
         /dev/vx/dsk/sfsdg/ENM665-home    2%
         /dev/vx/dsk/sfsdg/ENM665-cron    5%
         /dev/vx/dsk/sfsdg/ENM665-amos    4%
     /dev/vx/dsk/sfsdg/ENM665-pmlinks1    4%
 /dev/vx/dsk/sfsdg/ENM665-no_rollback    4%
          /dev/vx/dsk/sfsdg/ENM665-pm1    4%
          /dev/vx/dsk/sfsdg/ENM665-pm2    4%
      /dev/vx/dsk/sfsdg/ENM665-cust_fs    5%
         /dev/vx/dsk/sfsdg/ENM665-dlms    4%
 /dev/vx/dsk/sfsdg/ENM665-upgrade_ind    5%
      /dev/vx/dsk/sfsdg/ENM665-netlog    8%
 /dev/vx/dsk/sfsdg/ENM665-brsadm_home    6%
         /dev/vx/dsk/sfsdg/ENM665-data    4%
/dev/vx/dsk/sfsdg/ENM665-storobs_home    6%
         /dev/vx/dsk/sfsdg/ENM665-smrs    4%
        /dev/vx/dsk/sfsdg/ENM665-batch    3%
       /dev/vx/dsk/sfsdg/ENM665-georep    4%
          /dev/vx/dsk/sfsdg/ENM665-mdt   27%
 /dev/vx/dsk/sfsdg/ENM665-spool_mails    2%
    /dev/vx/dsk/sfsdg/ENM665-ddc_data   42%
     /dev/vx/dsk/sfsdg/ENM665-tfd_cli    3%
-----------------------------------  ----
-------------------------------------  ----
               ieatrcxb3388
-------------------------------------  ----
                           FileSystem  Use%
-------------------------------------  ----
       /dev/mapper/vg_root-vg1_lv_root   27%
                                tmpfs    0%
         /dev/vx/dmp/emc_clariion0_6s1   21%
        /dev/mapper/vg_root-vg1_lv_var    5%
/dev/mapper/neo4j_vg-neo4j_vg_neo4j_fs    1%
         /dev/mapper/vg_app-vg2_lv_opt    3%
         /dev/mapper/vg_app-vg2_lv_etc    1%
/dev/mapper/vg_app-vg2_lv_var_ericsson    1%
-------------------------------------  ----
-------------------------------------  ----
               ieatrcxb3133
-------------------------------------  ----
                           FileSystem  Use%
-------------------------------------  ----
       /dev/mapper/vg_root-vg1_lv_root   14%
                                tmpfs    0%
                  /dev/mapper/mpathap1   12%
        /dev/mapper/vg_root-vg1_lv_var   19%
         /dev/mapper/vg_app-vg2_lv_etc    1%
         /dev/mapper/vg_app-vg2_lv_opt    2%
/dev/mapper/vg_app-vg2_lv_var_ericsson    1%
        /dev/mapper/vg_vmvg-vg3_lv_vms   47%
-------------------------------------  ----
-------------------------------------  ----
               ieatrcxb3529
-------------------------------------  ----
                            FileSystem  Use%
-------------------------------------  ----
        /dev/mapper/vg_root-vg1_lv_root   27%
                                 tmpfs    1%
         /dev/vx/dmp/emc_clariion0_15s1   21%
         /dev/mapper/vg_root-vg1_lv_var   10%
 /dev/mapper/neo4j_vg-neo4j_vg_neo4j_fs    1%
          /dev/mapper/vg_app-vg2_lv_opt    3%
          /dev/mapper/vg_app-vg2_lv_etc    1%
 /dev/mapper/vg_app-vg2_lv_var_ericsson    1%
/dev/vx/dsk/elasticsearch_vg/elastic_fs    4%
             /dev/vx/dsk/jms_vg/jms_fs    1%
  /dev/vx/dsk/postgresdb_vg/postgres_fs    7%
          /dev/vx/dsk/mysql_vg/mysql_fs    1%
-------------------------------------  ----
-------------------------------------  ----
               ieatrcxb3134
-------------------------------------  ----
                           FileSystem  Use%
-------------------------------------  ----
```

```
        /dev/mapper/vg_root-vg1_lv_root   14%
                                  tmpfs    0%
                    /dev/mapper/mpathap1   12%
         /dev/mapper/vg_root-vg1_lv_var   19%
         /dev/mapper/vg_vmvg-vg3_lv_vms   45%
          /dev/mapper/vg_app-vg2_lv_opt    2%
          /dev/mapper/vg_app-vg2_lv_etc    1%
  /dev/mapper/vg_app-vg2_lv_var_ericsson    1%
  ------------------------------------  ----
  ------------------------------------  ----
                ieatrcxb3300
  ------------------------------------  ----
                               FileSystem  Use%
  ------------------------------------  ----
        /dev/mapper/vg_root-vg1_lv_root   14%
                                  tmpfs    0%
                    /dev/mapper/mpathap1   12%
         /dev/mapper/vg_root-vg1_lv_var   20%
  /dev/mapper/vg_app-vg2_lv_var_ericsson    1%
          /dev/mapper/vg_app-vg2_lv_etc    1%
          /dev/mapper/vg_app-vg2_lv_opt    2%
         /dev/mapper/vg_vmvg-vg3_lv_vms   49%
  ------------------------------------  ----
  ------------------------------------  ----
                ieatrcxb3301
  ------------------------------------  ----
                               FileSystem  Use%
  ------------------------------------  ----
        /dev/mapper/vg_root-vg1_lv_root   14%
                                  tmpfs    0%
                    /dev/mapper/mpathap1   12%
         /dev/mapper/vg_root-vg1_lv_var   19%
          /dev/mapper/vg_app-vg2_lv_opt    2%
  /dev/mapper/vg_app-vg2_lv_var_ericsson    1%
         /dev/mapper/vg_vmvg-vg3_lv_vms   45%
          /dev/mapper/vg_app-vg2_lv_etc    1%
  ------------------------------------  ----
  ----------------------------------------  ----
                ieatrcxb3565
  ----------------------------------------  ----
                                 FileSystem  Use%
  ----------------------------------------  ----
           /dev/mapper/vg_root-vg1_lv_root   28%
                                    tmpfs    0%
             /dev/vx/dmp/emc_clariion0_18s1   21%
             /dev/mapper/vg_root-vg1_lv_var    4%
              /dev/mapper/vg_app-vg2_lv_opt    2%
     /dev/mapper/vg_app-vg2_lv_var_ericsson    1%
              /dev/mapper/vg_app-vg2_lv_etc    1%
     /dev/mapper/neo4j_vg-neo4j_vg_neo4j_fs    1%
  /dev/vx/dsk/versant_bur_vg/versant_bur_fs    1%
         /dev/vx/dsk/versant_vg/versant_fs   75%
  ----------------------------------------  ----
  ------------------------------------  ----
                ieatrcxb3566
  ------------------------------------  ----
                               FileSystem  Use%
  ------------------------------------  ----
        /dev/mapper/vg_root-vg1_lv_root   27%
                                  tmpfs    0%
         /dev/vx/dmp/emc_clariion0_21s1   21%
         /dev/mapper/vg_root-vg1_lv_var    4%
  /dev/mapper/neo4j_vg-neo4j_vg_neo4j_fs    1%
          /dev/mapper/vg_app-vg2_lv_opt    2%
  /dev/mapper/vg_app-vg2_lv_var_ericsson    1%
          /dev/mapper/vg_app-vg2_lv_etc    1%
  ------------------------------------  ----
Successfully Completed Node Filesystem Healthcheck
ENM FILESYSTEM HEALTHCHECK: PASSED
------------------------------------------------------------------------
CHECKING KEY LSB SERVICES IN THE DEPLOYMENT
------------------------------------------------------------------------
Checking Services...
  ------------  -----------  ------  ---------
        System      Service   State  Run Level
  ------------  -----------  ------  ---------
   ieatlms7522        httpd  ONLINE          3
   ieatlms7522         sshd  ONLINE          3
   ieatlms7522  mcollective  ONLINE          3
   ieatlms7522      postfix  ONLINE          3
```

```
   ieatlms7522       puppet  ONLINE          3
   ieatlms7522     cobblerd  ONLINE          3
   ieatlms7522    rhq-agent  ONLINE          3
   ieatlms7522          ddc  ONLINE          3
   ieatlms7522        litpd  ONLINE          3
  ieatrcxb3388         sshd  ONLINE          3
  ieatrcxb3388    rhq-agent  ONLINE          3
  ieatrcxb3388          vcs  ONLINE          3
  ieatrcxb3388       puppet  ONLINE          3
  ieatrcxb3388  mcollective  ONLINE          3
  ieatrcxb3388          ddc  ONLINE          3
  ieatrcxb3133         sshd  ONLINE          3
  ieatrcxb3133  mcollective  ONLINE          3
  ieatrcxb3133          vcs  ONLINE          3
  ieatrcxb3133       puppet  ONLINE          3
  ieatrcxb3133    rhq-agent  ONLINE          3
  ieatrcxb3133          ddc  ONLINE          3
  ieatrcxb3529         sshd  ONLINE          3
  ieatrcxb3529    rhq-agent  ONLINE          3
  ieatrcxb3529          vcs  ONLINE          3
  ieatrcxb3529       puppet  ONLINE          3
  ieatrcxb3529  mcollective  ONLINE          3
  ieatrcxb3529          ddc  ONLINE          3
  ieatrcxb3134         sshd  ONLINE          3
  ieatrcxb3134    rhq-agent  ONLINE          3
  ieatrcxb3134          vcs  ONLINE          3
  ieatrcxb3134       puppet  ONLINE          3
  ieatrcxb3134  mcollective  ONLINE          3
  ieatrcxb3134          ddc  ONLINE          3
  ieatrcxb3300         sshd  ONLINE          3
  ieatrcxb3300  mcollective  ONLINE          3
  ieatrcxb3300          vcs  ONLINE          3
  ieatrcxb3300       puppet  ONLINE          3
  ieatrcxb3300    rhq-agent  ONLINE          3
  ieatrcxb3300          ddc  ONLINE          3
  ieatrcxb3301         sshd  ONLINE          3
  ieatrcxb3301    rhq-agent  ONLINE          3
  ieatrcxb3301          vcs  ONLINE          3
  ieatrcxb3301       puppet  ONLINE          3
  ieatrcxb3301  mcollective  ONLINE          3
  ieatrcxb3301          ddc  ONLINE          3
  ieatrcxb3565         sshd  ONLINE          3
  ieatrcxb3565    rhq-agent  ONLINE          3
  ieatrcxb3565          vcs  ONLINE          3
  ieatrcxb3565       puppet  ONLINE          3
  ieatrcxb3565  mcollective  ONLINE          3
  ieatrcxb3565          ddc  ONLINE          3
  ieatrcxb3566         sshd  ONLINE          3
  ieatrcxb3566    rhq-agent  ONLINE          3
  ieatrcxb3566          vcs  ONLINE          3
  ieatrcxb3566       puppet  ONLINE          3
  ieatrcxb3566  mcollective  ONLINE          3
  ieatrcxb3566          ddc  ONLINE          3
  ------------  -----------  ------  ---------
Service Status: PASSED
Successfully Completed Service Healthcheck
----------------------------------------------------------------------
CHECKING VCS CLUSTER SYSTEMS STATUS
----------------------------------------------------------------------
Beginning VCS Cluster System Healthcheck
INFO: 8 peer nodes found.
  ------------  -------  -----------  ------
        System    State      Cluster  Frozen
  ------------  -------  -----------  ------
  ieatrcxb3133  RUNNING  svc_cluster       -
  ieatrcxb3134  RUNNING  svc_cluster       -
  ieatrcxb3300  RUNNING  svc_cluster       -
  ieatrcxb3301  RUNNING  svc_cluster       -
  ieatrcxb3388  RUNNING   db_cluster       -
  ieatrcxb3529  RUNNING   db_cluster       -
  ieatrcxb3565  RUNNING   db_cluster       -
  ieatrcxb3566  RUNNING   db_cluster       -
  ------------  -------  -----------  ------
ENM VCS Cluster System Status: PASSED
Successfully Completed VCS Cluster System Healthcheck
----------------------------------------------------------------------
CHECKING VCS SERVICE GROUP STATUS
----------------------------------------------------------------------
Beginning VCS Service Group Healthcheck
Getting groups from cluster svc_cluster on system ieatrcxb3133
```

```
Getting groups from cluster db_cluster on system ieatrcxb3388
  -----------  --------------------------------------------------  ------------  --------------    →
-----------  ------------  ----------  ------
      Cluster                                                 Group        System           HAType    →
ServiceType  ServiceState  GroupState  Frozen
  -----------  --------------------------------------------------  ------------  --------------    →
-----------  ------------  ----------  ------
  svc_cluster                          Grp_CS_svc_cluster_flsserv  ieatrcxb3300        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                          Grp_CS_svc_cluster_flsserv  ieatrcxb3134        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                           Grp_CS_svc_cluster_cmserv  ieatrcxb3300        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                           Grp_CS_svc_cluster_cmserv  ieatrcxb3301        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                         Grp_CS_svc_cluster_nodeplugins  ieatrcxb3133        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                         Grp_CS_svc_cluster_nodeplugins  ieatrcxb3134        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                          Grp_CS_svc_cluster_nodecli  ieatrcxb3133        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                          Grp_CS_svc_cluster_nodecli  ieatrcxb3134        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                        Grp_CS_svc_cluster_itservices  ieatrcxb3133        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                        Grp_CS_svc_cluster_itservices  ieatrcxb3134        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                           Grp_CS_svc_cluster_uiserv  ieatrcxb3133        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                           Grp_CS_svc_cluster_uiserv  ieatrcxb3134        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                              Grp_CS_svc_cluster_sso  ieatrcxb3300        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                              Grp_CS_svc_cluster_sso  ieatrcxb3301        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                          Grp_CS_svc_cluster_msapgfm  ieatrcxb3133        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                          Grp_CS_svc_cluster_msapgfm  ieatrcxb3134        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                             Grp_CS_svc_cluster_dlms  ieatrcxb3300        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                             Grp_CS_svc_cluster_dlms  ieatrcxb3301        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                  Grp_CS_svc_cluster_fmalarmprocessing  ieatrcxb3133        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                  Grp_CS_svc_cluster_fmalarmprocessing  ieatrcxb3300        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                  Grp_CS_svc_cluster_fmalarmprocessing  ieatrcxb3301        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                  Grp_CS_svc_cluster_fmalarmprocessing  ieatrcxb3134        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                           Grp_CS_svc_cluster_mssnmpcm  ieatrcxb3133        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                           Grp_CS_svc_cluster_mssnmpcm  ieatrcxb3134        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                         Grp_CS_svc_cluster_pkiraserv  ieatrcxb3300        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                         Grp_CS_svc_cluster_pkiraserv  ieatrcxb3301        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                              Grp_CS_svc_cluster_said  ieatrcxb3300        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                              Grp_CS_svc_cluster_said  ieatrcxb3301        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                           Grp_CS_svc_cluster_nbfmsnmp  ieatrcxb3300        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                           Grp_CS_svc_cluster_nbfmsnmp  ieatrcxb3301        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                              Grp_CS_svc_cluster_mscm  ieatrcxb3133        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                              Grp_CS_svc_cluster_mscm  ieatrcxb3300        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                              Grp_CS_svc_cluster_mscm  ieatrcxb3301        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                              Grp_CS_svc_cluster_mscm  ieatrcxb3134        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                            Grp_CS_svc_cluster_mscmapg  ieatrcxb3133        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                            Grp_CS_svc_cluster_mscmapg  ieatrcxb3300        parallel    →
         vm         ONLINE          OK       -
  svc_cluster                            Grp_CS_svc_cluster_mscmapg  ieatrcxb3301        parallel    →
```

```
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_mscmapg  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                        Grp_CS_svc_cluster_haproxy_sb  ieatrcxb3133  active-standby    →
       lsb        ONLINE          OK       -
svc_cluster                        Grp_CS_svc_cluster_haproxy_sb  ieatrcxb3134  active-standby    →
       lsb       OFFLINE          OK       -
svc_cluster                         Grp_CS_svc_cluster_lvsrouter  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                         Grp_CS_svc_cluster_lvsrouter  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                         Grp_CS_svc_cluster_lvsrouter  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                         Grp_CS_svc_cluster_lvsrouter  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                               Grp_CS_svc_cluster_fmx  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                               Grp_CS_svc_cluster_fmx  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_lcmserv  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_lcmserv  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                        Grp_CS_svc_cluster_solrautoID  ieatrcxb3133  active-standby    →
        vm        ONLINE          OK       -
svc_cluster                        Grp_CS_svc_cluster_solrautoID  ieatrcxb3301  active-standby    →
        vm       OFFLINE          OK       -
svc_cluster                             Grp_CS_svc_cluster_mspm  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                             Grp_CS_svc_cluster_mspm  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                             Grp_CS_svc_cluster_mspm  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                             Grp_CS_svc_cluster_mspm  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                        Grp_CS_svc_cluster_accesscontrol  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                        Grp_CS_svc_cluster_accesscontrol  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                     Grp_CS_svc_cluster_eventbasedclient  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                     Grp_CS_svc_cluster_eventbasedclient  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                           Grp_CS_svc_cluster_httpd  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                           Grp_CS_svc_cluster_httpd  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_pmserv  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_pmserv  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                        Grp_CS_svc_cluster_nbalarmirp  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                        Grp_CS_svc_cluster_nbalarmirp  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                         Grp_CS_svc_cluster_openidm  ieatrcxb3300  active-standby    →
        vm        ONLINE          OK       -
svc_cluster                         Grp_CS_svc_cluster_openidm  ieatrcxb3301  active-standby    →
        vm       OFFLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_wpserv  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_wpserv  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                        Grp_CS_svc_cluster_impexpserv  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                        Grp_CS_svc_cluster_impexpserv  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_secserv  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_secserv  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_mspmip  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_mspmip  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                         Grp_CS_svc_cluster_vaultserv  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                         Grp_CS_svc_cluster_vaultserv  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                      Grp_CS_svc_cluster_pmrouterpolicy  ieatrcxb3300        parallel    →
```

```
        vm        ONLINE          OK       -
svc_cluster                  Grp_CS_svc_cluster_pmrouterpolicy  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                     Grp_CS_svc_cluster_smrsserv  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                     Grp_CS_svc_cluster_smrsserv  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_sps  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_sps  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_sps  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                          Grp_CS_svc_cluster_sps  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                       Grp_CS_svc_cluster_mscmce  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                       Grp_CS_svc_cluster_mscmce  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                       Grp_CS_svc_cluster_mscmce  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                       Grp_CS_svc_cluster_mscmce  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                  Grp_CS_svc_cluster_flowautomation  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                  Grp_CS_svc_cluster_flowautomation  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                   Grp_CS_svc_cluster_haproxy_ext  ieatrcxb3300  active-standby    →
       lsb        ONLINE          OK       -
svc_cluster                   Grp_CS_svc_cluster_haproxy_ext  ieatrcxb3301  active-standby    →
       lsb       OFFLINE          OK       -
svc_cluster                       Grp_CS_svc_cluster_mscmip  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                       Grp_CS_svc_cluster_mscmip  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                   Grp_CS_svc_cluster_haproxy_int  ieatrcxb3133  active-standby    →
       lsb        ONLINE          OK       -
svc_cluster                   Grp_CS_svc_cluster_haproxy_int  ieatrcxb3134  active-standby    →
       lsb       OFFLINE          OK       -
svc_cluster                   Grp_CS_svc_cluster_domainproxy  ieatrcxb3300  active-standby    →
        vm        ONLINE          OK       -
svc_cluster                   Grp_CS_svc_cluster_domainproxy  ieatrcxb3301  active-standby    →
        vm       OFFLINE          OK       -
svc_cluster                    Grp_CS_svc_cluster_shmcoreserv  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                    Grp_CS_svc_cluster_shmcoreserv  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                    Grp_CS_svc_cluster_cmutilities  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                    Grp_CS_svc_cluster_cmutilities  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                    Grp_CS_svc_cluster_kpicalcserv  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                    Grp_CS_svc_cluster_kpicalcserv  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                       Grp_CS_svc_cluster_supervc  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                       Grp_CS_svc_cluster_supervc  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                   Grp_CS_svc_cluster_visinamingsb  ieatrcxb3300  active-standby    →
        vm        ONLINE          OK       -
svc_cluster                   Grp_CS_svc_cluster_visinamingsb  ieatrcxb3301  active-standby    →
        vm       OFFLINE          OK       -
svc_cluster                      Grp_CS_svc_cluster_medrouter  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                      Grp_CS_svc_cluster_medrouter  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                   Grp_CS_svc_cluster_visinamingnb  ieatrcxb3133  active-standby    →
        vm        ONLINE          OK       -
svc_cluster                   Grp_CS_svc_cluster_visinamingnb  ieatrcxb3134  active-standby    →
        vm       OFFLINE          OK       -
svc_cluster                         Grp_CS_svc_cluster_solr  ieatrcxb3133  active-standby    →
        vm        ONLINE          OK       -
svc_cluster                         Grp_CS_svc_cluster_solr  ieatrcxb3134  active-standby    →
        vm       OFFLINE          OK       -
svc_cluster                    Grp_CS_svc_cluster_dpmediation  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                    Grp_CS_svc_cluster_dpmediation  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                         Grp_CS_svc_cluster_saserv  ieatrcxb3300        parallel    →
```

```
        vm        ONLINE          OK       -
svc_cluster                                  Grp_CS_svc_cluster_saserv  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                   Grp_CS_svc_cluster_netex  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                   Grp_CS_svc_cluster_netex  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_msnetlog  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_msnetlog  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                 Grp_CS_svc_cluster_kpiserv  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                 Grp_CS_svc_cluster_kpiserv  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_cmevents  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_cmevents  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                 Grp_CS_svc_cluster_mskpirt  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                 Grp_CS_svc_cluster_mskpirt  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                             Grp_CS_svc_cluster_comecimpolicy  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                             Grp_CS_svc_cluster_comecimpolicy  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_nedoserv  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_nedoserv  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                  Grp_CS_svc_cluster_fmserv  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                  Grp_CS_svc_cluster_fmserv  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                  Grp_CS_svc_cluster_fmserv  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                  Grp_CS_svc_cluster_fmserv  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                    Grp_CS_svc_cluster_msfm  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                    Grp_CS_svc_cluster_msfm  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                    Grp_CS_svc_cluster_msfm  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                    Grp_CS_svc_cluster_msfm  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                 Grp_CS_svc_cluster_ipsmserv  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                 Grp_CS_svc_cluster_ipsmserv  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                  Grp_CS_svc_cluster_shmserv  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                  Grp_CS_svc_cluster_shmserv  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                     Grp_CS_svc_cluster_msap  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                     Grp_CS_svc_cluster_msap  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_fmhistory  ieatrcxb3133        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_fmhistory  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_fmhistory  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_fmhistory  ieatrcxb3134        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_dchistory  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_dchistory  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                              Grp_CS_svc_cluster_msosssnmpfm  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                              Grp_CS_svc_cluster_msosssnmpfm  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                   Grp_CS_svc_cluster_apserv  ieatrcxb3300        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                   Grp_CS_svc_cluster_apserv  ieatrcxb3301        parallel    →
        vm        ONLINE          OK       -
svc_cluster                                Grp_CS_svc_cluster_bnsiserv  ieatrcxb3300        parallel    →
```

```
          vm        ONLINE          OK       -
  svc_cluster                          Grp_CS_svc_cluster_bnsiserv  ieatrcxb3301        parallel    →
          vm        ONLINE          OK       -
  svc_cluster                          Grp_CS_svc_cluster_mssnmpfm  ieatrcxb3133        parallel    →
          vm        ONLINE          OK       -
  svc_cluster                          Grp_CS_svc_cluster_mssnmpfm  ieatrcxb3300        parallel    →
          vm        ONLINE          OK       -
  svc_cluster                          Grp_CS_svc_cluster_mssnmpfm  ieatrcxb3301        parallel    →
          vm        ONLINE          OK       -
  svc_cluster                          Grp_CS_svc_cluster_mssnmpfm  ieatrcxb3134        parallel    →
          vm        ONLINE          OK       -
   db_cluster              Grp_CS_db_cluster_jms_clustered_service  ieatrcxb3388  active-standby    →
          lsb       OFFLINE          OK       -
   db_cluster              Grp_CS_db_cluster_jms_clustered_service  ieatrcxb3529  active-standby    →
          lsb        ONLINE          OK       -
   db_cluster            Grp_CS_db_cluster_mysql_clustered_service  ieatrcxb3388  active-standby    →
          lsb       OFFLINE          OK       -
   db_cluster            Grp_CS_db_cluster_mysql_clustered_service  ieatrcxb3529  active-standby    →
          lsb        ONLINE          OK       -
   db_cluster  Grp_CS_db_cluster_modeldeployment_cluster_service_1  ieatrcxb3565  active-standby    →
          lsb        ONLINE          OK       -
   db_cluster  Grp_CS_db_cluster_modeldeployment_cluster_service_1  ieatrcxb3566  active-standby    →
          lsb       OFFLINE          OK       -
   db_cluster         Grp_CS_db_cluster_postgres_clustered_service  ieatrcxb3388  active-standby    →
          lsb       OFFLINE          OK       -
   db_cluster         Grp_CS_db_cluster_postgres_clustered_service  ieatrcxb3529  active-standby    →
          lsb        ONLINE          OK       -
   db_cluster    Grp_CS_db_cluster_elasticsearch_clustered_service  ieatrcxb3388  active-standby    →
          lsb       OFFLINE          OK       -
   db_cluster    Grp_CS_db_cluster_elasticsearch_clustered_service  ieatrcxb3529  active-standby    →
          lsb        ONLINE          OK       -
   db_cluster           Grp_CS_db_cluster_opendj_clustered_service  ieatrcxb3388        parallel    →
          lsb        ONLINE          OK       -
   db_cluster           Grp_CS_db_cluster_opendj_clustered_service  ieatrcxb3529        parallel    →
          lsb        ONLINE          OK       -
   db_cluster         Grp_CS_db_cluster_sg_neo4j_clustered_service  ieatrcxb3529        parallel    →
          lsb        ONLINE          OK       -
   db_cluster         Grp_CS_db_cluster_sg_neo4j_clustered_service  ieatrcxb3566        parallel    →
          lsb        ONLINE          OK       -
   db_cluster         Grp_CS_db_cluster_sg_neo4j_clustered_service  ieatrcxb3565        parallel    →
          lsb        ONLINE          OK       -
   db_cluster        Grp_CS_db_cluster_versant_clustered_service_1  ieatrcxb3565  active-standby    →
         mixed       ONLINE          OK       -
   db_cluster        Grp_CS_db_cluster_versant_clustered_service_1  ieatrcxb3566  active-standby    →
         mixed       OFFLINE         OK       -
  -----------  --------------------------------------------------  ------------  --------------    →
-----------  ------------  ----------  ------
Healthcheck status: FAILED.
There appears to be a fault with the one or more VCS Service Groups.
```

2. Clear any faulted VCS service groups and bring them online manually.

    a. Log on to a peer server and change to the `root` user.

    b. Check the output from the `enm_healthcheck.sh` script for any VCS service group with the `ServiceState` property set to `OFFLINE|FAULTED`.

    c. Clear a faulted VCS service group, where *<service group name>* represents the name of the VCS service group and *<system>* represents the system name:

    ```
    hagrp -clear <service group name> -sys <system>
    ```

    d. Bring the VCS service group online:

    ```
    hagrp -online <service group name> -sys <system>
    ```

3. Make sure that all the parallel VCS service groups are online:

    a. Determine if a VCS service group is a parallel service group by checking the `standby` and `node_list` properties of the corresponding `vcs-clustered-service` in the LITP model.

    For example, run the following command to view the `name`, `standby` and `node_list` properties of the VCS service groups:

```
[root@ieatlms4616 bin]# litp show -p /deployments/enm/clusters/svc_ →
cluster/services/flsserv/
/deployments/enm/clusters/svc_cluster/services/flsserv
    type: vcs-clustered-service
    state: Applied
    properties:
        name: flsserv
        standby: 0
        node_list: svc-1,svc-2
        offline_timeout: 300
        active: 2
        online_timeout: 600
        dependency_list: lvsrouter
    children:
        /triggers
        /runtimes
        /applications
        /ha_configs
        /ipaddresses
        /filesystems
[root@ieatlms4616 bin]#
```

    b. Check that all the parallel service groups from the `enm_healthcheck.sh` output in Step 1 are online.

    If any parallel service group is offline, bring it online as follows:

```
hagrp -online <service group name> -sys <system>
```

5.7 Unmount or Mount Fails When Running restore_snapshot Command

Perform this procedure if a process is holding a file handle to an `NFS` mount during rollback and leaving it unmountable or /ericsson/tor/data failed to mount..

Prerequisites

— The rollback command `./enm_snapshots.bsh --action restore_snapshot` has failed with an error message similar to the following:

```
2017-12-29 09:12:16.089 ERROR umount                        : Failed to un-m →
ount /ericsson/tor/data
Traceback (most recent call last):
  File "/opt/ericsson/enminst/lib/import_iso.py", line 214, in umount
    exec_process(cmd)
  File "/opt/ericsson/enminst/lib/h_util/h_utils.py", line 148, in exec_proc →
```

```
ess
    raise IOError(process.returncode, stdout, command)
IOError: [Errno 16] umount2: Device or resource busy
umount.nfs: /ericsson/tor/data: device is busy
umount2: Device or resource busy
umount.nfs: /ericsson/tor/data: device is busy
: ['umount', '-f', '/ericsson/tor/data']
```

— Or /ericsson/tor/data failed to mount with an error message similar to the following:

```
Oct 21 17:06:53 ieatylms684 enminst ERROR mount : Failed to mount /ericsson/ →
tor/data#012Traceback (most recent call last):#012 File "/opt/ericsson/enmin →
st/lib/import_iso.py", line 183, in mount#012 exec_process
(cmd)#012 File "/opt/ericsson/enminst/lib/h_util/h_utils.py", line 201, in e →
xec_process#012 raise IOError(process.returncode, stdout, command)#012IOErro →
r: [Errno 32] mount.nfs: Connection timed out#012: ['mount', '/ericsson/tor/ →
data']
```

Steps

1. Proceed to step 4 if the problem is /ericsson/tor/data failed to mount, otherwise go to next step.

   Note: Resolve the root cause of the mount failure before powering on blades and re-running the rollback command.

2. Determine if there are processes preventing the `umount` command from completing.

   ```
   lsof <affected file system>
   ```

   In the preceding example, `/ericsson/tor/data` is the file system affected.

3. End each process that is holding resources on the affected file system using either the `pkill` or `kill` command.

   ```
   pkill <target_process>
   ```

   Or

   ```
   kill <PID>
   ```

4. Ensure all peer blades are fully powered on via the HP iLo:

   a. Log on to the HP iLo web interface for each blade.

   b. Navigate to the **Server Power** tab in the **Power Management** menu. If the server reports a status of **System Power: OFF**, click **Momentary Press** to power it on.

5. Rerun the rollback command:

```
./enm_snapshots.bsh --action restore_snapshot
```

The expected result is as follows:

```
ENM restore_snapshot finished successfully.
```

5.8 Copying VM Images to Nodes Fails

Use the steps described in this procedure if a plan failure occurs as VM images fail to copy to a node or several nodes.

Prerequisites

The installation plan has failed with an error message similar to the following:

```
2017-09-12 15:06:02 INFO  monitorinfo                  : SHOW_PLAN END
2017-09-12 15:06:02 INFO  monitorinfo                  : The plan has failed, f →
ailed tasks are:
2017-09-12 15:06:02 INFO  monitorinfo                  : Phase-96
2017-09-12 15:06:02 INFO  monitorinfo                  : Task: Failed
2017-09-12 15:06:02 INFO  monitorinfo                  :   Item: /deployments/e →
nm/clusters/svc_cluster/services/mssnmpfm/applications/vm-service_mssnmpfm
2017-09-12 15:06:02 INFO  monitorinfo                  :   Info: Copy VM image  →
file
2017-09-12 15:06:02 INFO  monitorinfo                  :         "ERICrhel6jbos →
simage_CXP9031560-2.35.5.qcow2" to node
2017-09-12 15:06:02 INFO  monitorinfo                  :         "enm01svc02" f →
or instance "mssnmpfm" as part of VM
2017-09-12 15:06:02 INFO  monitorinfo                  :         deploy

..

2017-09-12 15:06:02 INFO  monitorinfo                  : Total Phases: 275 | Ac →
tive Phase(s): - | PlanState: Failed | TotalTasks: 7877 | Initial: 208 | Running →
: 0 | Success: 7641 | Failed: 28 | Stopped: 0
2017-09-12 15:06:02 ERROR deploy                       : An error occurred runn →
ing ENM Deployment
```

Steps

1. Execute the `litp create_plan` and `litp run_plan` commands:

   ```
   litp create_plan
    litp run_plan
   ```

2. When the plan starts, you can monitor the upgrade progress in a separate terminal instance using the following command:

   ```
   watch litp show_plan -a
   ```

3. After the plan has completed continue with the tasks described in the *Post Install Actions* section of ENM Installation Instructions.

If the plan fails again, contact local Ericsson support.

5.9 View the GRUB Boot Sequence on the Serial Console

The GRand Unified Bootloader (GRUB) boot sequence output is not available to view from the serial console. Cobbler does not configure `grub.conf` to direct GRUB outputs towards the serial console. To see a GRUB boot sequence entirely from the serial console you need to manually edit the `grub.conf` file on the Management Server (MS) and also on each of the peer nodes.

Prerequisites

You have `root` user access to the MS and Peer Nodes.

Steps

1. Log on to the ENM MS as the **`litp-admin`** user and switch to the **`root`** user.
2. Find out which Teletype (TTY) is being used as the serial console.

   Depending on the hardware being used, it may either be `ttyS0` or `ttyS1`.

   a. In a new terminal window, log on to the iLO using SSH and start the virtual serial port (VSP).

   ```
   </>hpiLO-> vsp
   Virtual Serial Port Active: COM1
   Starting virtual serial port.
   Press 'ESC (' to return to the CLI Session.
   ```

   b. On the MS, run the following commands:

   ```
   echo test > /dev/ttyS0
   echo test > /dev/ttyS1
   ```

   c. After each command, check the VSP to see which TTY is being used. If `test` is displayed on the VSP after the first command, then `ttyS0` is used. If it is displayed after the second command, then `ttyS1` is used.
3. On the MS, change to the directory of the `grub.conf` file:

   ```
   cd /boot/grub/
   ```
4. Back up the `grub.conf` file and save it with the date:

   ```
   cp grub.conf "grub.conf.backup-$(date +%F_%R)"
   ```
5. Open the `grub.conf` file:

```
vim grub.conf
```

6. Apply the following changes to the file:

    a. Ensure that these two lines are present at the start of the file, above the title section:

    ```
    serial --speed=115200
    terminal --timeout=5 console serial
    ```

    b. Update the `kernel` parameter of the title section of the file.

    — If `ttyS0` is used as the serial console, ensure the following parameters are present:

    ```
    console=tty00 console=ttyS0,115200
    ```

    — If `ttyS1` is used as the serial console, ensure the following parameters are present:

    ```
    console=tty00 console=ttyS1,115200
    ```

    The following is an example of the `grub.conf` file after the applied changes:

    Example

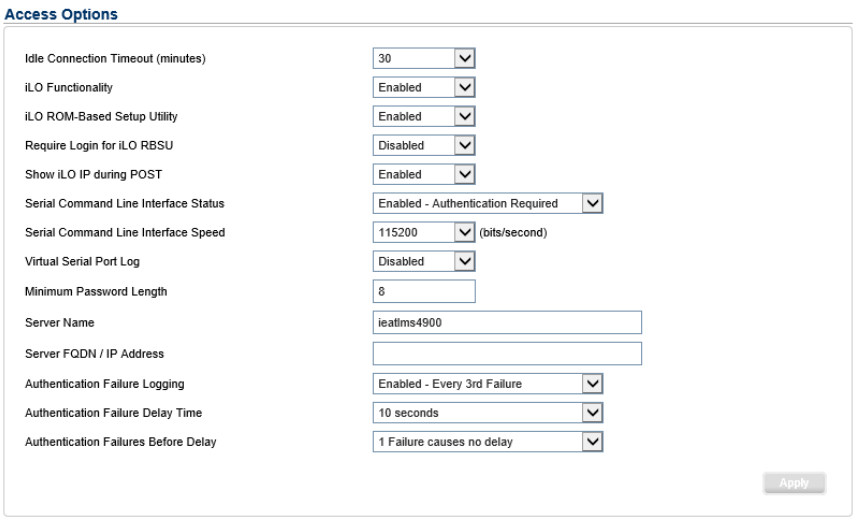
    ```
    # grub.conf generated by anaconda
    #
    # Note that you do not have to rerun grub after making changes to t →
    his file
    # NOTICE:  You have a /boot partition.  This means that
    #          all kernel and initrd paths are relative to /boot/, eg.
    #          root (hd0,0)
    #          kernel /vmlinuz-version ro root=/dev/mapper/vg_root-vg1_ →
    lv_root
    #          initrd /initrd-[generic-]version.img
    #boot=/dev/mpathb
    default=0
    timeout=10
    splashimage=(hd0,0)/grub/splash.xpm.gz
    hiddenmenu
    password --encrypted $1$VscjuyK8$9UuYHrnJ0VEGjKQ/Yeac50
    serial --speed=115200
    terminal --timeout=5 serial console
    title Red Hat Enterprise Linux 6 (2.6.32-504.62.1.el6.x86_64)
            root (hd0,0)
            kernel /vmlinuz-2.6.32-504.62.1.el6.x86_64 ro root=/dev/map →
    per/vg_root-vg1_lv_root rd_NO_LUKS LANG=en_US.UTF-8 rd_NO_MD  KEYTA →
    BLE=us rd_LVM_LV=vg_root/vg1_lv_swap SYSFONT=latarcyrheb-sun16 cras →
    hkernel=auto rd_LVM_LV=vg_root/vg1_lv_root rd_NO_DM rhgb quiet cons →
    ole=tty00 console=ttyS0,115200
            initrd /initramfs-2.6.32-504.62.1.el6.x86_64.img
    ```

7. Verify the Serial Command Line Interface Speed parameter is set to the same speed value as in the `grub.conf` file.

    a. Log on to the iLO in your browser.

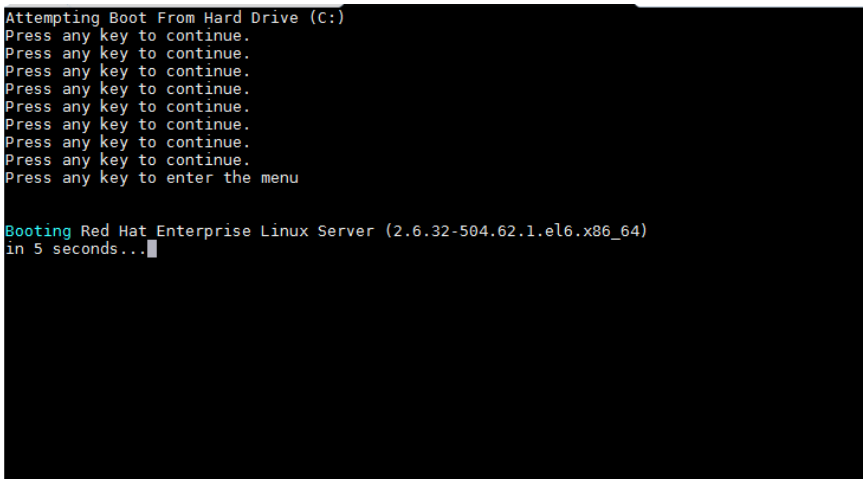
    b. Navigate to the **Access Settings** tab in the Administration menu.

c. Ensure that the `115200` value is selected from the drop-down menu for the `Serial Command Line Interface Speed` parameter.



8. Reboot the MS.

   a. On the serial console, press any key during this sequence to access the GRUB boot menu.



9. If the GRUB boot menu is not accessible on the serial console, restore the backup created in Step 4, and repeat Steps 5 to 8.

10. Log on to each of the peer nodes as the `litp-admin` user, switch to the **`root`** user, and run the commands specified in Steps 2 to 7.

Results

You can see and use the GRUB boot menu on the serial console.

5.10 Storage FS List Command from clish Returns Empty

Solution

If the `storage fs list` command from clish returns empty with no result, then restart the `vxdcli` service.

1. Check the status of `vxdcli` service on both the NAS nodes and verify if the lock files are present.

```
[root@VA_01_01 log]# /opt/VRTSsfmh/etc/vxdcli.sh status
RESTARTING
Check lock dir /var/vx/dcli/vxdcli.sh.lock
```

2. Check if the lock file is present in the `/var/vx/dcli` directory on both NAS nodes.

   Example

```
[root@nas414415_01 ~]# cd /var/vx/dcli/
[root@nas414415_01 dcli]# ls -lrt
total 4
drwxr-xr-x. 2 root root 4096 Aug 30 02:48 log
-rw-r--r--  1 root root    0 Aug 30 10:10 vxdcli.sh.lock
```

3. Remove the lock file if present.

```
[root@nas414415_01 ~]# rm -rf /var/vx/dcli/vxdcli.sh.lock
```

4. Stop and start the `vxdcli` service on each node.

   a. Stop the `vxdcli` service.

```
[root@nas414415_01 ~]# /opt/VRTSsfmh/etc/vxdcli.sh stop
[root@nas414415_01 ~]# /opt/VRTSsfmh/etc/vxdcli.sh status
STOPPED
```

   b. Start the `vxdcli` service.

```
[root@nas414415_01 ~]# /opt/VRTSsfmh/etc/vxdcli.sh start
[root@nas414415_01 ~]# /opt/VRTSsfmh/etc/vxdcli.sh status
RUNNING
```

5.11 Remove LVM Snapshots that Cause Rescue Mode Boot Error

If booting to `rescue` mode, with Red Hat 6.10 and an LVM snapshot exists that includes additional text in the name compared to the original Logical volume name, the following error is displayed.

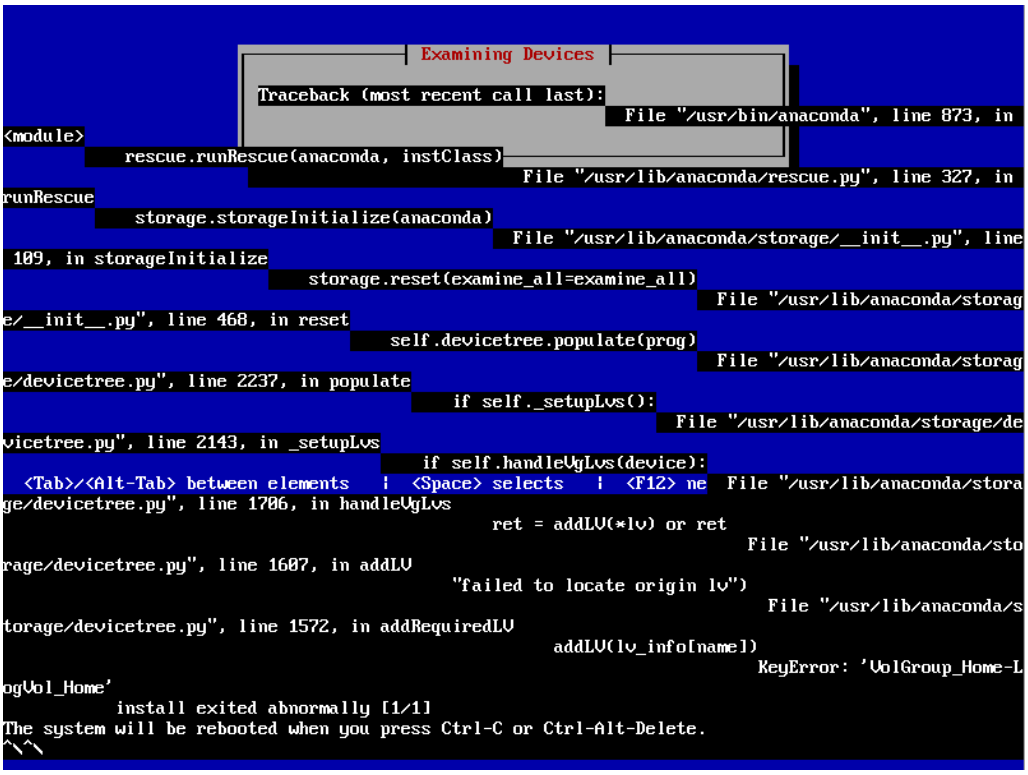


Figure 1 Error Message

Solution

To resolve the issue, do the following steps.

1. Boot the server into **rescue** mode.
2. Select **Rescue installed system** from the menu options.

Figure 2 Rescue Installed System

3. Select **Skip** from the **Rescue** menu.

Figure 3 Rescue Menu

4. Select the **Start shell** option.

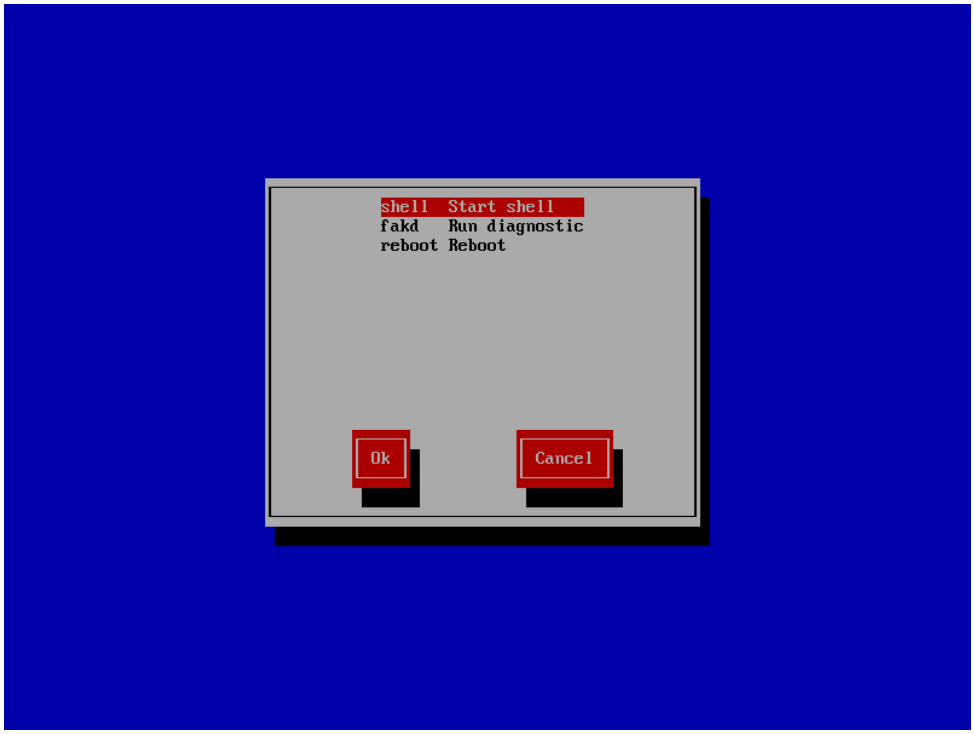


Figure 4 Start Shell

5. Run the following command in the shell.

```
# lvscan
inactive '/dev/VolGroup_root/LogVol_Root' [9.50 GiB] inherit
inactive Original '/dev/VolGroup_Home/LogVol_Home' [152.00 MiB] inherit
inactive Snapshot '/dev/VolGroup_Home/ANY_LogVol_Home' [152.00 MiB] inherit
inactive '/dev/VolGroup_swap/LogVol_Swap' [1020.00 MiB] inherit
```

6. Check for all snapshots that match the original Logical volume name but have additional text. In the previous example, the original Logical volume is `LogVol_Home` and the snapshot with the additional text is `ANY_LogVol_Home`.

```
inactive Snapshot '/dev/VolGroup_Home/ANY_LogVol_Home' [152.00 MiB] inherit
```

7. Remove the snapshots that match the original Logical volume name but have the additional text in the name.

```
# lvremove /dev/VolGroup_Home/ANY_LogVol_Home
Logical volume "ANY_LogVol_Home" successfully removed
```

8. Reboot the system and try the **`Rescue installed system`** again.

```
# reboot
```

9. Confirm that the Root File System is mounted as the `/mnt/sysimage` directory.
10. Continue with the analysis in `rescue` mode.

5.12 Troubleshooting sshd Service in VA

> sshd services may fail to start after Veritas Access installation.

Prerequisite

— Integrated Lights-Out (iLO) access to the nodes.

— Root access to NAS nodes.

Solution

1. Log on to the NAS node using putty and verify the `ssh_keys` file permissions.

```
nas414415_01:~ # ll /etc/ssh/
rw-r----. 1 root polkitd 227 Jan 24 07:18 ssh_host_ecdsa_key
rw-r----. 1 root polkitd 387 Jan 24 07:18 ssh_host_ed25519_key
rw-r----. 1 root polkitd 1679 Jan 24 07:18 ssh_host_rsa_key
```

2. Check the status of the Veritas cluster.

```
[root@nas414415_01 .ssh]# vxclustadm nidmap
Name CVM Nid CM Nid State
nas414415_01 0 0 Joined: Master
nas414415_02 1 1 Out of Cluster
```

3. If ssh_keys group ownership in *step 1* is different than `root`, change it as `root`. To change this permissions, log on to the server using iLO console.

```
nas414415_02  # chown :root ssh_host_ecdsa_key
nas414415_02  # chown :root ssh_host_ed25519_key
nas414415_02  # chown :root ssh_host_rsa_ke
```

```
nas414415_02:~ # ll /etc/ssh/
rw-r----. 1 root root 227 Jan 24 07:18 ssh_host_ecdsa_key
rw-r----. 1 root root 387 Jan 24 07:18 ssh_host_ed25519_key
rw-r----. 1 root root 1679 Jan 24 07:18 ssh_host_rsa_key
```

4. Disable the SELinux.

```
nas414415_02:~ # vi /etc/selinux/config
SELINUX=disabled
```

5. Restart the sshd service.

```
nas414415_02:~ # service sshd restart
```

6. Reboot the NAS node which is out of the cluster.

```
nas414415_02:~ # reboot
```

Both the nodes joined the cluster.

```
[root@nas414415_01 .ssh]# vxclustadm nidmap
Name CVM Nid CM Nid State
nas414415_01 1 1 Joined: Master
nas414415_02 0 0 Joined: Slave
```

5.13 Troubleshooting mntlock Service in VA

Cause

The following mntlock error message occurs after running the rollback snapshots post an upgrade failure.

```
Unable to unmount a VCS locked file-system in CVM/CFS environment
Error Message
UX:vxfs umount: ERROR: V-3-26420: file system not mount locked
UX:vxfs umount: ERROR: V-3-26388: file system
```

Solution

1. Collect the output of the following commands for debugging.

```
# service portmap status
# service portmap status
# service nfs status
# hastatus -sum
```

2. Follow the section *ENM NAS Data Collection Overview* from ENM Data Collection Guideline to collect coredump.

   Note: Coredump will crash the node. Coredump must be collected only when the root cause needs to be identified. In other scenarios, skip this step and proceed to *step 3*.

3. Log on to the NAS node with support user.

```
# su - support
```

4. Set the mount lock for the problem volume.

```
# /usr/lib/fs/vxfs/fsadm -F vxfs -o mntlock=VCS  <File System>
```

5. Unmount the volume forcefully.

```
# /opt/VRTS/bin/umount -f -o mntunlock=VCS <File System>
```

6. If the `umount` command is unsuccessful in *step 5*, proceed with the following `vxumount` command.

```
# /opt/VRTS/bin/vxumount -f -o mntunlock=VCS <File System>
```

5.14 ENM Healthcheck Failures Due to File System Exceeding the Usage Threshold

5.14.1 /dev/mapper/vg_root-vg1_lv_vms Exceeds 80% Usage

Perform this procedure if ENM healthcheck fails because `/dev/mapper/vg_root-vg1_lv_vms` exceeds 80% usage on any peer node.

The following output indicates that a file system has exceeded the 80% usage threshold:

```
[root@cloud-ms-1 bin]# ./enm_healthcheck.sh --action node_fs_healthcheck
Beginning ENM pre-Healthchecks
Node Status: PASSED
Completed ENM pre-Healthchecks
Checking if peer node filesystems do not exceed
90% for NAS
92% for versnt-neo4j, elasticsearch
80% for all other filesystem
Obtaining NAS information from the LITP model
Fileystems exceed usage:
Host 'cloud-svc-1' filesystem(s) '/dev/mapper/vg_root-vg1_lv_vms' exceed 80% usa →
ge
```

Solution

1. Log on to the hosts exceeding 80% usage.

```
mount | grep /dev/mapper/vg_root-vg1_lv_vms
```

If the output is similar to the following example, you must clean up the instances directory.

```
dev/mapper/vg_root-vg1_lv_vms on /var/lib/libvirt/instances
type ext4 (rw,nobarrier)
```

2. Clean up the affected directories.

```
cd /var/lib/libvirt/instances/
find . -maxdepth 2 -type d -name "last_undefined_vm" -exec rm -vrf {} \;
```

   Repeat this step for all the listed servers.

3. Log on the MS again and perform a health check of the ENM deployment.

```
cd /opt/ericsson/enminst/bin
./enm_healthcheck.sh --action node_fs_healthcheck
```

   Output similar to the following indicates that the ENM deployment is healthy and you can perform an ENM upgrade now.

```
[root@ieatlms7522 bin]# ./enm_healthcheck.sh --action node_fs_healthcheck
Beginning ENM pre-Healthchecks
Node Status: PASSED
Completed ENM pre-Healthchecks
Checking if peer node filesystems do not exceed
90% for NAS
92% for versnt-neo4j, elasticsearch
80% for all other filesystems
Obtaining NAS information from the LITP model
Successfully Completed Node Filesystem Healthcheck
```

   On some occasions, the removal of the last_undefined_vm images from the affected host still causes a health check to fail because the (qcow2) sparse disk images do not shrink when disk space is not used anymore. If the health check fails again at the same stage, proceed with the next steps.

4. Lock the affected node, where `cloud-svc-1` is name listed as node with filesystem `/dev/mapper/vg_root-vg1_lv_vms` exceeding 80% usage from health check.

```
[root@ms-1 ~]# cd /opt/ericsson/enminst/bin/
[root@ms-1 bin]# ./vcs.bsh --lock -s cloud-svc-1
INFO: 6 peer nodes found.
2019-11-11 11:11:11.001 INFO  lock                          : Locking cloud-svc-1
2019-11-11 11:11:11.111 INFO  lock                          : System cloud-svc-1 lockin →
g
```

5. Log on to the affected node and list `virsh` instances directories size. List all the virsh VMs to check if they are in `shut off` state.

```
[root@ms-1 bin]# ssh litp-admin@cloud-svc-1
[litp-admin@cloud-svc-1 ~]$ su -
[root@cloud-svc-1 ]# cd /var/lib/libvirt/instances
[root@cloud-svc-1]# du -sh *
1.6G    apserv
44K     domainproxy
2.0G    ipsmserv
1.5G    kpicalcserv
1.5G    kpiserv
1.5G    lcmserv
16K     lost+found
1.7G    lvsrouter
4.2G    mspm
1.4G    pmserv
2.7G    scripting
```

```
3.7G    shmcoreserv
44K     solrautoID
1.6G    sps
1.7G    visinamingnb


[root@cloud-svc-1 ~]# virsh list --all
Id    Name                           State
----------------------------------------------------
 -     apserv                         shut off
 -     ipsmserv                       shut off
 -     kpicalcserv                    shut off
 -     kpiserv                        shut off
 -     lcmserv                        shut off
 -     lvsrouter                      shut off
 -     mspm                           shut off
 -     pmserv                         shut off
 -     scripting                      shut off
 -     shmcoreserv                    shut off
 -     sps                            shut off
 -     visinamingnb                   shut off
```

6. Execute the undefine procedure for each VM consuming the highest amount of disk space. The undefined VM is gone from `virsh` list.

```
[root@cloud-svc-1 ~]# virsh undefine shmcoreserv
[root@cloud-svc-1 ~]# virsh list --all
Id    Name                           State
----------------------------------------------------
 -     apserv                         shut off
 -     ipsmserv                       shut off
 -     kpicalcserv                    shut off
 -     kpiserv                        shut off
 -     lcmserv                        shut off
 -     lvsrouter                      shut off
 -     mspm                           shut off
 -     pmserv                         shut off
 -     scripting                      shut off
 -     shmcoreserv                    shut off
 -     sps                            shut off
 -     visinamingnb                   shut off
```

Note: When a VM is undefined, its system logs are removed.

7. Log out from a node back to LMS and unlock the node when all the VMs consuming a high amount of disk space are undefined.

```
[root@cloud-svc-1 ~]# exit
logout
[litp-admin@cloud-svc-1 ~]$ exit
logout
Connection to cloud-svc-1 closed.
[root@ms-1 ~]# cd /opt/ericsson/enminst/bin/
[root@ms-1 bin]# ./vcs.bsh --unlock -s cloud-svc-1
2019-11-13 11:33:11.415 INFO  unlock                        : Unlocking clou →
d-svc-1
2019-11-13 11:33:12.696 INFO  unlock                        : System cloud-s →
vc-1 unlocking.
```

8. Repeat *Step 1* to *Step 3* once the output from the following command is empty.

```
[root@ms-1 bin]# ./vcs.bsh --groups | grep svc-1 | grep Invalid
```

5.14.2 /dev/mapper/vg_root-lv_software Exceeds 80% Usage

Perform this procedure if ENM healthcheck fails because `/dev/mapper/vg_root-lv_software` exceeds 80% usage.

Cause

If there is a significant difference in the output between the **df** and the **du** commands, then this issue is probably caused by an ISO used during a previous upgrade, which was not detached from the loop devices.

Solution

Before running the steps, ensure the following prerequisites are met.

— The healthcheck fails and indicates that `/dev/mapper/vg_root-lv_software` file system is almost full.

```
Fileystems exceed usage:
Host 'cloud-ms-1' filesystem(s) '/dev/mapper/vg_root-lv_software' exceed 80% usage
```

— There is a difference in the output between the `df` and the `du` commands.

In the following example, the **df** command output shows `39G` used and the **du** command shows `27G` used.

```
[root@cloud-ms-1 autoDeploy]# df -hT /software
Filesystem                          Type  Size  Used Avail Use% Mounted on
/dev/mapper/vg_root-lv_software     ext4   50G   39G   7.7G  84% /software
```

```
[root@cloud-ms-1 autoDeploy]# du -sh /software/
27G /software/
```

1. List all systems attached to the loop devices.

```
[root@cloud-ms-1 autoDeploy]# losetup -a
```

Example

```
[root@cloud-ms-1 autoDeploy]# losetup -a
/dev/loop0: [fd06]:917510 (/software/autoDeploy/ERICenm_CXP9027091-1.85.57.iso)
```

2. List the files and directories under the `/software` volume. The ISO from the output of the previous step is not listed under the `/software` volume as shown in the following example:

Example

```
[root@cloud-ms-1 autoDeploy]# ll -ha /software/autoDeploy/

total 27G
drwxr-xr-x.  4 root root 4.0K Jan 24 14:09 .
drwxr-xr-x.  4 root root 4.0K Jan 21 20:46 ..
-rw-r--r--.  1 root root 4.5G Jan 24 14:03 big.iso
drwxr-xr-x.  6 root root 4.0K Jan 21 21:04 deploy
-rw-r--r--.  1 root root 5.4M Jan 21 21:09 deployment-description-slices-1.86.5-SNAPSHO →
T.zip
-rw-r--r--.  1 root root  61M Jan 21 21:04 DeploymentScripts-2.0.164.tar.gz
-rw-r--r--.  1 root root  13G Jan 21 20:49 ERICenm_CXP9027091-1.87.57.iso
-rw-r--r--.  1 root root 5.1M Jan 21 21:09 ERICenmdeploymenttemplates_CXP9031758-1.86.5 →
-SNAPSHOT.zip
-rw-r--r--.  1 root root 823M Jan 21 20:46 ERIClitp_CXP9024296-2.109.5.iso
-rw-r--r--.  1 root root 8.0K Jan 21 21:19 IPMICloudHelperTool-1.0.14.rpm
-rw-r--r--.  1 root root  170 Jan 21 21:05 lastIsoImportedDoNotDelete
-rw-r--r--.  1 root root  77K Jan 21 21:19 MASTER_siteEngineering.txt
-rw-r--r--.  1 root root 4.5G Jan 21 20:47 RHEL76_OS_Patch_Set_CXP9037739-1.4.1.iso
-rw-r--r--.  1 root root 4.1G Jan 21 20:47 RHEL_OS_Patch_Set_CXP9034997-2.7.1.iso
drwxr-xr-x. 13 root root 4.0K Jan 21 21:09 slices
-rw-------.  1 root root 1.7K Jan 22 06:52 vm_private_key
-rw-r--r--.  1 root root 3.5K Jan 22 07:11 vmware-install.log
```

3. Remove the loop device that is pointing to the non-existing ISO on the `/software` volume where `<loop device>` is the loop device identified in *step 1*.

```
[root@cloud-ms-1 autoDeploy]# losetup -d <loop device>
```

Example

```
[root@cloud-ms-1 autoDeploy]# losetup -d /dev/loop0
```

4. Verify the attached loop devices.

```
[root@cloud-ms-1 autoDeploy]# losetup -a
```

5. Verify the disk usage.

```
[root@cloud-ms-1 autoDeploy]# df -hT /software
Filesystem                          Type  Size  Used Avail Use% Mounted on
/dev/mapper/vg_root-lv_software     ext4   50G   27G   21G  57% /software
```

Result: The ENM Healthcheck does not report that disk usage is exceeded for the `/software` volume.

6 Trouble Shooting Tasks for OpenStack Based Deployments

This section describe the tasks for OpenStack based deployments.

6.1 Recover ENM after Cloud Infrastructure Outage

> This section describes how to use the Recover ENM Workflow to resolve issues with the ENM on Cloud after an cloud infrastructure outage. Cloud infrastructure issues such as network interruptions and slow storage may prevent functioning of ENM applications.

Cloud infrastructure issues such as network interruptions and slow storage may prevent functioning of ENM applications.

Solution

The Recover ENM Workflow can reconstitute all the VMs in the vENM tenancy, which can resolve any hidden application issues after an infrastructure outage. Recover ENM workflow builds a deployment view of vENM from the information in `enm.json`. The workflow builds recovery phases for all the VMs in order of priority.

All ENM VMs in the tenancy are reconstituted by triggering HA workflow sequentially for each phase internally.

Note:
- At any given point in time, only one VM of a particular type is reconstituted.
- ENM applications can suffer minimal downtime during the workflow execution.

Ensure that the following prerequisites are met:

- No ongoing lifecycle operations running in the tenancy such as Upgrade, Snapshot, Rollback, Backup, Restore before the Recover ENM workflow is triggered.
- No active instances of High Availability Workflow exist.
- The underlying cloud infrastructure is stable.
- All ENM VMs are available in consul member view and OpenStack cloud. If any member is missing in either consul or OpenStack cloud, Recover ENM workflow ends at the Build Recovery Phases stage.
- VNF-LCM UI is available.

1. Open the VNF-LCM UI in the browser, using the URL http://%3Cexternal_ip_for_services_vm%3E/index.html#workflows.

   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.

2. Select the **Recover ENM** workflow, then click **Start a New Instance**. Alternatively, right-click **Recover ENM** workflow and select **Start a New Instance**.

3. Choose if the current state underlying cloud infrastructure is stable by answering **Yes** or **No**.

   Note: If **No** is selected, the workflow ends immediately.

4. Monitor the Recover ENM Workflow. Use the **refresh** option to reload and check the progress of the workflow instance. The High Availability workflow within the Recovery workflow is triggered multiple times based on the ENM configuration. The progress remains at 30% until all the phases of recovery is completed.

5. Multiple HA workflows are triggered as a part of recovery workflow internally and their progress can be checked at runtime by clicking on the **High Availability** block.

6. Wait for the completion of the Recover ENM workflow.

7. Multiple instances of High Availability workflow are triggered sequentially for each phase and can be seen in the main page of VNF-LCM UI.

6.1.1 Failure or Canceling Recover ENM Workflow

If the Recover ENM workflow fails or it is manually canceled, run the following procedure to manually enable High Availability (HA).

Steps

1. Run the below command to check if HA is disabled from VNF-LCM as root user.

   ```
   # consul kv get enm/applications/availability_manager/services/sam/disable_h →
   a
   ```

   Example

   ```
   [root@vnflaf-services-0 cloud-user]# consul kv get enm/applications/availabi →
   lity_manager/services/sam/disable_ha
   true
   ```

2. If the output of the command is `true`, then run the following command to enable HA.

```
# consul kv delete enm/applications/availability_manager/services/sam/disabl
e_ha
```

Example

```
[root@vnflaf-services-0 cloud-user]# consul kv delete enm/applications/avail
ability_manager/services/sam/disable_ha
Success! Deleted key: enm/applications/availability_manager/services/sam/dis
able_ha
```

6.2 Troubleshooting High Availability for vENM

This section describes how to troubleshoot failures related to High Availability (HA) for vENM. For an overview of the vENM HA solution, refer to section *ENM on Cloud HA Solution* in ENM Product Description - [Reference 25].

6.2.1 High Availability Recovery of VMs

> This section describes the procedure to recover VMs when a High Availability Workflow fails to recover VMs.

Prerequisites

— Any underlying infrastructure issue that has caused VMs to fail to recover is resolved. If an infrastructure issue is suspected, contact your cloud administrator.

— A client machine with a `Keystone.rc` and tenancy `<keypair>.pem` file, which must use same credential used during initial install of the ENM system.

Diagnostics

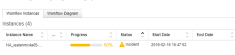
High Availability Workflow has number of states and some of the states require recovery procedures that are to be executed.

Steps mentioned in the Table 1 require navigation through the VNF-LCM ENM GUI.

Note: The table also includes successful states.

Table 1 High Availability Workflow State

High Availability Workflow State	How to Identify	Description	Action
Completed with success	In the **Workflow Diagram**(1), workflow completed at end event labeled `Workflow finished`	The workflow has successfully recovered all VMs.	None

High Availability Workflow State	How to Identify	Description	Action
	`successfully`. 		
Completed early with no VMs	In the **Workflow Diagram**(1), workflow completed at end event labeled `Workflow finished with no VMs`. 	The workflow has omitted all VMs because they are handled by another workflow.	None
Completed after Camunda error	In the **Workflow Diagram**(1), workflow completed at end event labeled `Workflow failed to recover VMs`.  .	The workflow has encountered an unhandled Camunda error and is unable to continue.	1. Resolve any underlying infrastructure issue. 2. Run the General Recovery Procedure on page 51.
Completed with failure	In the **Workflow Diagram**(1), workflow completed at end event labeled `Workflow finished with Failure`.  .	The workflow has reached the end of its retry limit (1000 retries, about 21 days) and it is not able to recover the VMs. This is likely due to an infrastructure issue and HA is unable to recover the VMs without manual intervention.	1. Resolve any underlying infrastructure issue. 2. Run the General Recovery Procedure on page 51.
Long-running	In the **High Availability Workflow** (2) page, workflow is colored green, **Status** in `Progress`, and the **Start Date** is at least 30 minutes in advance. 	The workflow is still attempting to recover VMs. It has not yet reached the end of its retry limit (1000 retries, about 21 days). A long running HA is likely due to an infrastructure issue and HA is unable to recover the VMs without manual intervention.	1. Follow the High Availability Workflow is Unable to Delete Inner Stacks on page 53. The steps also detail how to identify the deletion failure. 2. If the workflow is still unable to complete, contact Ericsson Support.
Failed with incident	In the **High Availability Workflow** page(2), workflow is colored orange and has **Status** `Incident`. 	The workflow has encountered an unexpected exception and is unable to continue.	1. Cancel the workflow by clicking **Cancel Execution**. 2. Resolve any underlying infrastructure issue. 3. Run the General Recovery Procedure on page 51.
Incorrectly canceled	In the **High Availability Workflow** page(2),	The workflow is manually canceled on the VNF Life Cycle	If the workflow is incorrectly canceled:

High Availability Workflow State	How to Identify	Description	Action
	workflow is colored Grey and has **Status** `Cancelled`. 	Manager (VNF-LCM) application. Workflow may be correctly canceled and no action is required unless issues still persist.	1. Resolve any underlying infrastructure issue. 2. Run the General Recovery Procedure on page 51.

(1) To navigate to the **Workflow Diagram**:

1 Launch VNF Life Cycle Manager (VNF-LCM) application.

2 On the **VNF Life Cycle Manager** page, double-click **High Availability Workflow**.

3 Under the Workflow Instances tab, double-click the workflow in question. The diagram is displayed at the bottom of the page.

(2) To navigate to the **High Availability Workflow**:

1 Launch VNF Life Cycle Manager (VNF-LCM) application.

2 On the **VNF Life Cycle Manager** page, double-click **High Availability Workflow**.

6.2.2 General Recovery Procedure

> This section describes the procedure to initiate the High Availability Workflow for unrecoverable VMs.

Prerequisites

— The VNF-LCM services and dB VMs must be alive in consul and reachable.

— The VNF-LCM GUI is functioning.

— At least two sevicereg VMs must be alive in consul and reachable.

Solution

1. From the **High Availability Workflow** page, double-click the workflow in question.
2. Click the **Workflow Log** tab.
3. Take a note of the failed VMs by searching for log `Health check failed for VMs`. The matching log indicates the failing VMs. For example, the following log identifies two VMs.

   Example

   ```
   Health check failed for VMs: {"ieatenmc6b03-comecimpolicy-0":"10.10.0.62","i
   eatenmc6b03-medrouter-1":"10.10.0.110"}
   ```

   Make a note of the VMs and their IP addresses.

4. Connect to the emp instance from the client machine and switch to root user where <emp_external_ip_list> is the external IP address associated to the emp instance. The IP can be found in the SED.

   If emp is not available, **ssh** into the vnflaf services instance instead.

   ```
   # ssh -i <key_name>.pem cloud-user@<emp_external_ip_list>
   [cloud-user@emp ~]$
   [cloud-user@emp ~]$ sudo -i
   [root@emp ~]#
   ```

5. Search the Consul members list for each of the failed VMs identified from *step 1*. If they are in a left state or if they are not found, they need to be recovered in the later steps.

   ```
   [root@emp ~]# consul members | grep -i "ieatenmc6b03-comecimpolicy-0\|ieatenmc6b03-medr →
   outer-1"
   ieatenmc6b03-comecimpolicy-0      10.10.0.228:8301  left    client  0.9.2  2         dc →
   1
   ```

   In the above example, ieatenmc6b03-comecimpolicy-0 is in a left state and ieatenmc6b03-medrouter-1 is not found. Therefore, both must be recovered.

   Note: If all VMs identified from *step 1* exist in the output and none of them are in a left state, then all the VMs have managed to recover. No further action is needed after this procedure.

6. Identify the High Availability workflow name with the highest version by curling vnflaf-serivces/wfs/rest/definitions.

   ```
   [root@emp ~]$ curl -s http://vnflaf-services/wfs/rest/definitions |
   grep -o enmdeploymentworkflows[0-9.-]*HighAvailabilityWorkflow__top | sort --version-so →
   rt | tail -1
   ```

   The output looks like the following:

   ```
   enmdeploymentworkflows.--.1.66.11.-.HighAvailabilityWorkflow__top
   ```

7. Start a High Availability Workflow by running the following command.

   ```
   curl --header "Content-Type: application/json; charset=utf-8" -X POST --data '{
            "definitionId":"<HA workflow name>",
            "businessKey":"<Unique identifier>",
            "variables": {
                "vms": {
                     "type":"String",
                     "value":"{\"<VM_1 name>\":\"<VM_1 IP address>\",\"<VM_2 name>\":\"<VM →
   _2 IP>\"}"
                }
           }
       }' http://vnflaf-services/wfs/rest/instances
   ```

   In the command:

— HA workflow name is identified from *step 6.*

— Unique identifier is user-generated string fewer than 255 characters to aid the troubleshooting. For example, `HA_manual_1`

— VM names and VM IP addresses are identified from *step 5*. In this example, there are two failed VMs. There may be a scenario with two or more failed VMs. Adjust the query parameters accordingly by adding fewer or more `\"<VM name>\":\"<VM IP address>\"`, separated by commas.

Example

```
[root@emp ~]$ curl -i --header "Content-Type: application/json; charset=utf-8" -X POST
--data '{"definitionId":"enmdeploymentworkflows.--.1.87.2.--.HighAvailabilityWorkflow__
top","businessKey":"HA_manual_1","variables":{"vms":{"type":"String","value":"{\"ieaten
mc4a05-uiserv-0\":\"10.10.1.92\",
\"ieatenmc4a05-neo4j-0\":\"10.10.1.48\"}"}}}' http://vnflaf-services/wfs/rest/instances
```

Result: The HTTP response contains status 201.

```
HTTP/1.1 201 Created
Date: Wed, 28 Aug 2019 14:59:43 GMT
Server: Apache-Coyote/1.1
Content-Type: application/json
Via: 1.1 enmapache.athtem.eei.ericsson.se
Cache-Control: no-cache
Transfer-Encoding: chunked

{"instanceId":"77ef94a3-c9a4-11e9-8653-fa163ed7ac0f","businessKey":"HA_manua
l_1","definitionId":"enmdeploymentworkflows.--.1.87.2.--.HighAvailabilityWor
kflow__top"}
```

8. Wait for the VMs to recover. Depending on the type of VMs being recovered, the network speed, the state of the ENM system and other factors, it may take from a few minutes to a few hours for VMs to recover. High Availability Workflows may run during this time. Progress can be monitored from the VNF Life Cycle Manager (VNF-LCM) GUI.
9. If VMs are still unable to recover, contact Ericsson Support.

6.2.3 High Availability Workflow is Unable to Delete Inner Stacks

6.2.3.1 Identify the Issue

> The following steps use the OpenStack command line client to identify if a HA workflow is unable to recover due to an inner stack being in a `DELETE_FAILED` state.

Prerequisites

— The VNF-LCM services and dB VMs must be 'alive' in Consul and reachable.

— The VNF-LCM GUI is functioning.

— At least two sevicereg VMs must be 'alive' in Consul and reachable.

1. Identify all the VMs undergoing the HA workflow.

    a. Open the ENM Application Launcher in a browser. Under the **Provisioning** section, click **VNF Life Cycle Manager (VNFLCM)**.

    b. Double click **High Availability Workflow**.

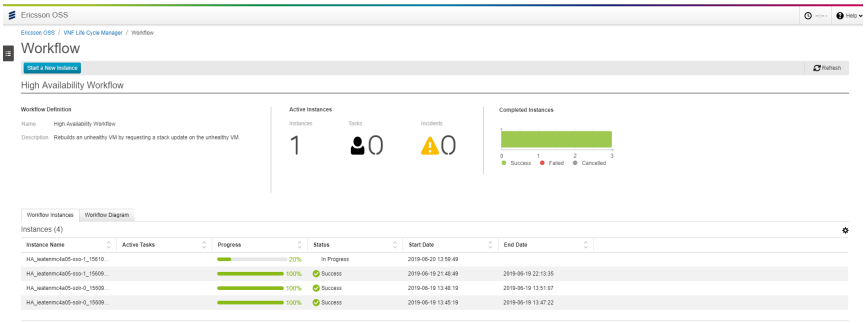


Figure 5 High Availability Workflow

Result: Displays a list of HA workflows.

    c. Click the title of the **Progress** column to sort the workflows by progress status. Take a note of any HA workflow that is active and the progress is below 100%.

    d. Double-click on a workflow that is in progress and then click the **Workflow Log** tab to see the logs. Take a note of the VM names and their relevant IP addresses in the workflow. If there are more VMs, expand the log to see the full list by clicking on the arrow **>** to the left of the log entry.

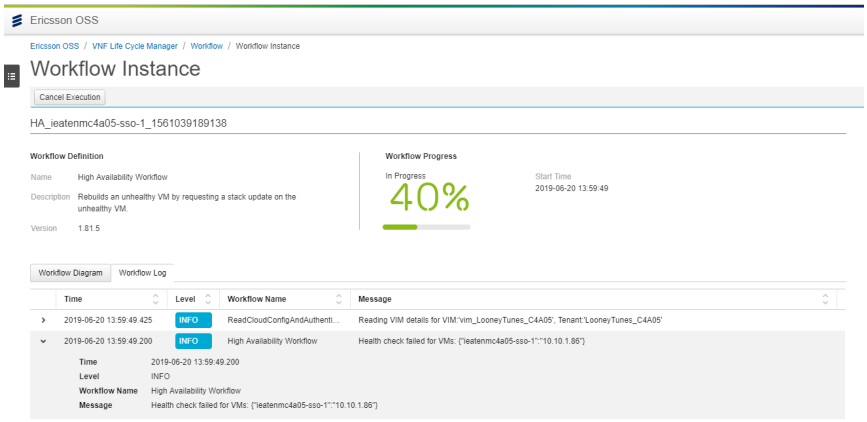


Figure 6 Workflow Instance

Follow the same steps for each workflow that is in progress.

2. Find the inner stacks associated with the VMs.

   VM names are in the following format `<project-name>-<service-group-name>-<VM-number>`.

   For example, for VM `ieatenmc4a05-sso-0`, `ieatenmc4a05` corresponds to the project name, `sso` corresponds to the service group and `0` is the VM number.

   Set the following variables by substituting the `<service-group-name>` and the `<VM-number>` appropriately based on the VM names found in the previous step.

   ```
   sg_name="<service-group-name>"
   vm_number="<VM-number>"
   ```

   Note: There are exceptions to the VM naming convention `<project-name>-<service-group-name>-<VM-number>`. VMs of certain service groups do not use their exact service group name, but can be found as follows:

   ```
   - lvsrouter: ieatenmc4a05_lvs_8c148906-421d-4b88-bf87-9e05f519195b
   - servicereg: ieatenmc4a05_serviceregistry_1069c27c-c7e6-44c1-a06a-e4d8cd9f204a
   - nfsnrbk: ieatenmc4a11_nfsnorollback_c3453140-d8ce-4a86-9499-7d5e03f719fd
   - scp: ieatenmc4a11_scripting_6bd2a1d6-dca1-4cce-80c8-87212706ec0f
   - haproxy-int: ieatenmc4a11_haproxyint_df5dc678-3373-42ab-9867-c3f28152ba05
   - haproxy-sb: ieatenmc4a11_haproxysb_42d7c1c1-36a0-4ca6-8b0e-c8462d02b546
   ```

   For example, to find the status of the inner stack for `nfsnrbk` VMs, set sg_name as follows:

   ```
   [root@openstack-client ~]# sg_name="nfsnorollback"
   ```

Do!

To search the sentinel VM, the `vm_number` must be set to **0**:

```
[root@openstack-client ~]# sg_name="sentinel"
[root@openstack-client ~]# vm_number="0"
```

Run the following command to find status of the inner stack containing the VM:

```
openstack stack list | grep $sg_name | awk '{print $2}' | xargs openstack st
ack resource list -n2 |
awk -v vm="$vm_number" '$2 == vm' | awk '{print $4}' | xargs openstack stack
 show | grep stack_status
```

This command uses the variables that were set to find the correct stack.

```
[root@openstack-client ~]# sg_name="sso"
[root@openstack-client ~]# vm_number="1"
[root@openstack-client ~]# openstack stack list | grep "_${sg_name}_" | awk
'{print $2}' | xargs openstack stack resource list -n2 | awk -v vm="$vm_numb
er" '$2 == vm' | awk '{print $4}' | xargs openstack stack show | grep stack_
status
| stack_status          | CREATE_COMPLETE                                                |

                                                                                |
| stack_status_reason   | Stack CREATE completed successfully                            |

                                                                                |
```

Check that the inner stacks are in `DELETE_FAILED` state. If the stacks remain in this state, follow the instructions in the section "Recover ENM VMs in Delete Failed State" to recover any failed VMs.

6.2.3.2 Recover ENM VMs in a Delete Failed State

High Availability relies on core services in OpenStack and Consul to be functional. The following procedures describe the steps to be taken in such an event.

- Delete Inner Stack Resources on page 57
- Align Database on page 59
- Verification on page 59

Note: The steps in these procedures do not fix any configuration issue with the existing Cloud Infrastructure that may not be able to process requests sent from ENM.

Prerequisites

— Identify and fix any OpenStack infrastructure issues for OpenStack services to be fully operational and HA to proceed.

  The following symptoms are related to infrastructure issues:

  — Failure to delete or create a stack.

  — Time-outs or errors in sending requests to OpenStack API.

  — Time-outs or errors in receiving responses from OpenStack API.

  — A compute or controller node or both is down when they must be running.

  — VMs cannot communicate with one another. VMs go into a 'failed' state due to a failing Serf health check.

— Ensure that there are enough free resources in OpenStack to hold the recreated instances.

Stop!

Do not send any OpenStack requests to the heat API to create or delete stacks manually.

6.2.3.2.1 Delete Inner Stack Resources

Solution

The following steps use the OpenStack command line client and the ENM user interface to delete the resources of faulty inner stacks. The deletion of the server and port uses the OpenStack Nova and Neutron services respectively.

1. Set the following variables by substituting the `<service-group-name>` and the `<VM-number>` appropriately based on the VM names found in the *step 1* of Identify the Issue on page 53 section for HA workflow being unable to inner stacks.

   ```
   sg_name="<service-group-name>"
   vm_number="<VM-number>"
   ```

   Run the following command to find the resources of the inner stack containing the VM:

```
openstack stack list | grep "_${sg_name}_" | awk '{print $2}' |
xargs openstack stack resource list -n2 | awk -v vm="$vm_number" '$2 == vm'
| awk '{print $4}' | xargs -t openstack stack resource list
```

Example

```
[root@openstack-client ~]# sg_name="sso"
[root@openstack-client ~]# vm_number="1"
[root@openstack-client ~]# openstack stack list | grep "_${sg_name}_" | awk '{print $2}' | xargs op
enstack stack resource list -n2 | awk -v vm="$vm_number" '$2 == vm' | awk '{print $4}' | xargs -t o
penstack stack resource list
openstack stack resource list -n2 31282ebd-2318-487f-a0cd-e51cd50ca18f
+--------------------------------+--------------------------------------+------------------------+
----------------+--------------------+-------------------------------------------------------------+
| resource_name                  | physical_resource_id                 | resource_type          |
 resource_status | updated_time       | stack_name                                                  |
+--------------------------------+--------------------------------------+------------------------+
----------------+--------------------+-------------------------------------------------------------+
| sso_definition_interface1_port | fa3ed732-2df4-4a85-90d7-afe11a65c3f2 | OS::Neutron::Port      |
 CREATE_COMPLETE | 2019-06-17T16:36:50 | ieatenmc4a05_sso_3297ee06-15ba-4656-a8d0-                   |
|                                |                                      |                        |
                 |                     |      | -1ee25bd056ef-sso-alm3vr43kykt-1-jdtyrcq7e5cg               |
| sso_definition_vm              | 91939c76-7932-446f-8943-320b7462cd5d | OS::Nova::Server       |
 CREATE_COMPLETE | 2019-06-17T16:36:50 | ieatenmc4a05_sso_3297ee06-15ba-4656-a8d0-                   |
|                                |                                      |                        |
                 |                     |      | -1ee25bd056ef-sso-alm3vr43kykt-1-jdtyrcq7e5cg               |
| sso_definition_user_data       | a80910ac-abf3-4492-ae85-2fc715a85975 | OS::Heat::MultipartMime |
 CREATE_COMPLETE | 2019-06-17T16:36:50 | ieatenmc4a05_sso_3297ee06-15ba-4656-a8d0-                   |
|                                |                                      |                        |
                 |                     |      | -1ee25bd056ef-sso-alm3vr43kykt-1-jdtyrcq7e5cg               |
+--------------------------------+--------------------------------------+------------------------+
----------------+--------------------+-------------------------------------------------------------+
```

The command shows all the resources contained in the inner stack that HA is attempting to recover. Make a note of the physical resource IDs of the ports and the server. These are used to delete the inner stack resources. Similarly, note the inner stack ID printed as part of the `openstack stack resource list` command, as the ID is used to verify that HA has proceeded. In the example, the inner stack ID is `31282ebd-2318-487f-a0cd-e51cd50ca18f`.

2. Delete all the ports in the inner stack.

```
# openstack port delete <port-physical-resource-id>
```

Example

```
# openstack port delete fa3ed732-2df4-4a85-90d7-afe11a65c3f2
```

This command produces no output when successful. To confirm that the ports are deleted successfully, run the command:

```
# openstack port show <port-physical-resource-id>
```

Example

```
# openstack port show fa3ed732-2df4-4a85-90d7-afe11a65c3f2
```

The output contains an error message stating that the port is not found and confirming that it is deleted.

```
ResourceNotFound: No Port found for fa3ed732-2df4-4a85-90d7-afe11a65c3f2
```

3. Delete the server in the inner stack.

```
# openstack server delete <server-physical-resource-id>
```

Example

```
# openstack server delete 91939c76-7932-446f-8943-320b7462cd5d
```

This command produces no output when successful. To confirm that the servers are deleted successfully, run the command:

```
# openstack server show <server-physical-resource-id>
```

Example

```
# openstack server show 91939c76-7932-446f-8943-320b7462cd5d
```

The output contains an error message stating that the server does not exist and confirming that it is deleted successfully.

```
No server with a name or ID of '91939c76-7932-446f-8943-320b7462cd5d' exists.
```

4. Rerun the previous steps for all the VMs identified.

6.2.3.2.2 Align Database

Contact the OpenStack administrator to ensure that the inner stack resource state is consistent with the state of the inner stack in its database. Do not proceed if it is not aligned and the inner stack is not marked `DELETE_COMPLETE`.

6.2.3.2.3 Verification

Solution

The following step uses the OpenStack command line client to ensure that HA workflow is able to continue successfully.

1. Check if the inner stacks have `DELETE_COMPLETE` status. Use the inner stack ID acquired in *Step 1* of Delete Inner Stack Resources on page 57.

```
# openstack stack show <innerstack-id> | grep stack_status
```

```
[root@openstack-client ~]# openstack stack show 31282ebd-2318-487f-a0cd-e51cd50ca18f |
grep stack_status
| stack_status          | DELETE_COMPLETE
```

```
| stack_status_reason   | Stack DELETE completed successfully
```

HA Workflow automatically proceeds to mark the inner stacks unhealthy and then recover the failed VMs. The process can be monitored using the VNF-LCM user interface.

6.3 Trouble Shooting Network Viewer

6.3.1 Visualization of Topology Relationships in Network Viewer

> If an expected relationship line is not drawn between a RadioNode and a 5GRadioNode on the Network Viewer map, confirm whether the line should be visible or not.

Prerequisites

The user requires a `Cmedit_Operator` role to access the ENM CLI.

Note: The steps should be completed sequentially.

Steps

1. Ensure you have the highest zoom level on the geographical map.

   Due to the nature of an NR-NSA system, nodes can be situated only tens of meters away from each other on a geographical map. Therefore the line can be difficult to see unless fully zoomed in. You can also check it in the logical view. If a relationship line still cannot be seen, proceed to the next step.

2. Verify that both nodes have geographical coordinates. If either of them are without geographical coordinates, a relationship line is not drawn on the map. (It can be viewed in the logical view.)

3. Ensure the node types selected are eNodeB Baseband Radio Node and 5GRadioNode, as an X2 interface can only be configured between these.

   a. Open the ENM Application Launcher. Under Provisioning, open the Command-Line Interface (ENM CLI).

   b. Run either of the following commands for a 5GRadioNode:

      ```
      cmedit get <5GRadioNode_Name> ExternalENodeBFunction --namespace=GN →
      BCUCP
      ```

      or

```
cmedit get <5GRadioNode_Name> ExternalENodeBFunction --namespace=Nr →
atGNodeBFunction
```

Sample output of command:

```
FDN : someFdn
```

c. Verify that the output contains an FDN.

d. Run the following command for a eNodeB Baseband Radio Node:

```
cmedit get <eNodeB_Baseband_Radio_Node_Name> ENodeBFunction --names →
pace=lrat
```

Sample output of command:

```
FDN : someFdn
```

e. Verify that the output contains an FDN.

f. If the nodes in the command don't bring back an FDN or FDNs, they are of the wrong type and a relationship line is not drawn.

g. If the nodes in the command bring back FDNs, they are of the correct type. Proceed to the next step.

4. Check that the 5GRadioNode is synced.

   a. Open the ENM CLI and run the following command:

```
cmedit get <5GRadioNode_Name> --detailnode --netype=5GRadioNode
```

   Sample output of command:

```
FDN : someFdn
syncStatus : SYNCHRONIZED
```

   b. If the node is `UNSYNCHRONIZED`, ENM cannot assess whether there is an X2 link and a relationship line is not drawn.

   c. If the node is `SYNCHRONIZED`, proceed to the next step.

5. Check that the X2 interface is operational between the eNodeB Baseband Radio Node and the 5GRadioNode.

   a. Open the ENM CLI.

   b. Run the following command:

```
cmedit get <eNodeB_Baseband_Radio_Node_Name> TermPointToGNB.operati →
onalState
```

Sample output of command:

```
FDN : someFdn
operationalState : ENABLED
```

c. If `TermPointToGNB` doesn't exist or the operational state is `DISABLED`, there is no valid X2 link between the nodes.

d. If `TermPointToGNB` operational state is `ENABLED`, proceed with the next step.

6. Determine if the X2 interface is configured correctly on both the eNodeB Baseband Radio Node and 5GRadioNode side.

   a. Run the following command in the ENM CLI to find the configuration on the RadioNode side:

```
cmedit get <eNodeB_Baseband_Radio_Node_Name> ENodeBFunction.(enbid,
 enodebplmnid) -ns=lrat
```

   Sample output of command:

```
FDN : someFdn
eNBId : 1
eNodeBPlmnId : {mnc=50, mncLength=2, mcc=353}
```

   b. Run the following command in the ENM CLI to find the configuration on the 5GRadioNode side:

```
cmedit get <5GRadioNode_Name> ExternalENodeBFunction.(enodebid, enb
plmnid) -ns=GNBCUCP
```

   or

```
cmedit get <5GRadioNode_Name> ExternalENodeBFunction.(enodebid, enb
plmnid) -ns=NratGNodeBFunction
```

   Sample output of command:

```
FDN : someFdn
eNodeBId : 1
eNBPlmnId : 353:50
```

   Note: The eNBPlmnId in the above line denotes "MCC:MNC". Hence, 353 is the MCC value and 50 is the MNC value.

   c. Compare the values found for the eNBId and eNodeBPlmnId on eNodeB Baseband Radio Node side to the values found for the eNodeBId and eNBPlmnId of the 5GRadioNode.

eNodeB Baseband Radio Node	Comparison	5GRadioNode
eNBId	is equal to	eNodeBId
eNodeBPlmnId.mcc	is equal to	eNBPlmnId.mcc
eNodeBPlmnId.mnc	is equal to	eNBPlmnId.mnc

Tip: The above sample command outputs show a valid X2 link between the eNodeB Baseband Radio Node and 5GRadioNode, as the values for the specified attributes match.

eNodeB Baseband Radio Node	Comparison	5GRadioNode
eNBId value: 1	is equal to	eNodeBId value: 1
eNBPlmnId.mcc value: 353	is equal to	eNodeBPlmnId.mcc value: 353
eNBPlmnId.mnc value: 50	is equal to	eNodeBPlmnId.mnc value: 50

d. If these values are equal then a valid operational X2 link exists, and the relationship line should be drawn.

6.3.2 Check Visibility of X2-eNB-gNB Relationship Line between an eNodeB Baseband Radio Node and gNodeB Baseband Radio Node

> If an expected relationship line is not drawn between an eNodeB Baseband Radio Node and gNodeB Baseband Radio Node on the Network Viewer map, confirm whether the line should be visible or not.

Prerequisites

The user requires a `Cmedit_Operator` role to access the ENM CLI.

Note: The steps should be completed sequentially.

Steps

1. Ensure the highest zoom level on the geographical map.

   Because of the nature of an NR-NSA system, the nodes can be situated only tens of meters away from each other on the geographical map. Therefore the

line can be difficult to see unless fully zoomed in. (You can also check in the logical view.) If a relationship line cannot be seen, proceed to the next step.

2. Verify that both nodes have geographical coordinates. If either of them are without geographical coordinates, a relationship line is not drawn on the map. (It can be viewed in the logical view.)

3. Ensure the node types selected are eNodeB Baseband Radio Node and gNodeB Baseband Radio Node. An X2-eNB-gNB interface can be configured between these.

    a. Open the ENM Application Launcher.

    b. Under Provisioning, open the Command-Line Interface (ENM CLI).

    c. Run one of the following commands for gNodeB Baseband Radio Node:

    ```
    cmedit get <gNodeB_Baseband_Radio_Node_Name> ExternalENodeBFunction →
     --namespace=GNBCUCP
    ```

    or

    ```
    cmedit get <gNodeB_Baseband_Radio_Node_Name> ExternalENodeBFunction →
     --namespace=NratGNodeBFunction
    ```

    Result: Sample output

    ```
    FDN : someFdn
    ```

    d. Verify that the output contains one or more FDNs.

    e. Run the following command for an eNodeB Baseband Radio Node:

    ```
    cmedit get <eNodeB_Baseband_Radio_Node_Name> ENodeBFunction --names →
    pace=lrat
    ```

    Result: Sample output

    ```
    FDN : someFdn
    ```

    f. Verify that the output contains one or more FDNs.

    g. If the nodes in the command do not bring back an FDN, they are of the wrong type and a relationship line will not be drawn.

    h. If the nodes in the command bring back one or more FDNs, they are of the correct type. Proceed to the next step.

4. Check that the gNodeB Baseband Radio Node is synced.

    a. Open the ENM CLI and run the following command:

```
cmedit get <eNodeB_Baseband_Radio_Node_Name> --detailnode
```

Result: Sample output

```
FDN : someFdn
syncStatus : SYNCHRONIZED
```

b. If the node sync status is `UNSYNCHRONIZED`, ENM cannot assess whether there is an X2 link and the relationship line is not drawn.

c. If the node sync status is `SYNCHRONIZED`, proceed to the next step.

5. Check that the X2-eNB-gNB interface is operational between the eNodeB Baseband Radio Node and gNodeB Baseband Radio Node.

   a. Open the ENM CLI and run the following command:

```
cmedit get <eNodeB_Baseband_Radio_Node_Name> TermPointToGNB.operati →
onalState
```

   Result: Sample output

```
FDN : someFdn
operationalState : ENABLED
```

   b. If `TermPointToGNB` doesn't exist or if the operational state is disabled, then there is no valid X2-eNB-gNB link between the nodes and the relationship line is not drawn.

   c. If the `TermPointToGNB` operational state is `ENABLED`, proceed with the next step.

6. Determine if the X2-eNB-gNB interface is configured correctly on both the eNodeB Baseband Radio Node and gNodeB Baseband Radio Node side.

   a. Open the ENM CLI and run the following command to find the configuration on the eNodeB Baseband Radio Node side:

```
cmedit get <eNodeB_Baseband_Radio_Node_Name> ENodeBFunction.(enbid, →
 enodebplmnid) -ns=lrat
```

   Result: Sample output

```
FDN : someFdn
eNBId : 1
eNodeBPlmnId : {mnc=50, mncLength=2, mcc=353}
```

   b. Run one of the following commands in the ENM CLI to find the configuration on the gNodeB Baseband Radio Node side:

```
cmedit get <gNodeB_RadioNode_Name> ExternalENodeBFunction.(enodebid →
, enbplmnid) -ns=GNBCUCP
```

or

```
cmedit get <gNodeB_RadioNode_Name> ExternalENodeBFunction.(enodebid →
, enbplmnid) -ns=NratGNodeBFunction
```

Result: Sample output

```
FDN : someFdn
eNodeBId : 1
eNBPlmnId : 353:50
```

Note: `eNBPlmnId` in the above line denotes `mcc` : `mnc`. 353 is the `mcc` value and 50 is the `mnc` value.

c. Compare the values found for `eNBId` and `eNodeBPlmnId` on the eNodeB Baseband Radio Node side to the values found for the `eNodeBId` and `eNBPlmnId` of the gNodeB Baseband Radio Node. If these values are equal, then a valid operational X2-eNB-gNB link exists, and the relationship line should be drawn.

eNodeB Baseband Radio Node	Comparison	gNodeB Baseband Radio Node
eNBId	is equal to	eNodeBId
eNodeBPlmnId.mcc	is equal to	eNBPlmnId.mcc
eNodeBPlmnId.mnc	is equal to	eNBPlmnId.mnc

Tip: The above sample command outputs show a valid X2-eNB-gNB link between the eNodeB Baseband Radio Node and gNodeB Baseband Radio Node, as the values for the specified attributes match:

eNodeB Baseband Radio Node	Comparison	gNodeB Baseband Radio Node
eNBId value: 1	is equal to	eNodeBId value: 1
eNBPlmnId.mcc value: 353	is equal to	eNodeBPlmnId.mcc value: 353
eNBPlmnId.mnc value: 50	is equal to	eNodeBPlmnId.mnc value: 50

7 Troubleshooting Applications

This section describe the tasks for OpenStack based deployments.

7.1 Troubleshooting License Control and Monitor Service

This section provides troubleshooting steps to diagnose and fix common errors in the ENM License Control Monitor (LCM) service.

7.1.1 "Error 9999 : Internal Error Node ID ... Cannot add node due to invalid/ inadequate license" Error Message.

The license permission is checked internally if a user attempts to add a node to ENM as in the following example:

```
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
```

An error message appears if there is no valid license installed and the usage exceeds the capacity as in the following example:

```
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.
```

Steps

1. Check if the license file is already installed in the system:

   ```
   lcmadm list
   ```

   If the license file is already installed then the system returns an output as the following example:

   ```
   Capacity License Info
   Name         Expiry Date                 Limit Vendor Info
   FAT1023070   Feb 28 2016 23:59:59 GMT    100   Radio_Network_Base_Package_nu →
   mberOf_5MHzSC
   ```

2. Check the usage of license file already installed on the system:

   ```
   lcmadm list --current-usage
   ```

   If there is at least a installed license file currently in use then the system returns an output as the following example:

```
Name         Expiry Date                 Limit Usage       Usage Recorded     →
                Vendor Info
FAT1023070   Feb 28 2016 23:59:59 GMT    100   110         Nov 3 2015 16:00:  →
00 GMT          Radio_Network_Base_Package_numberOf_5MHzSC
```

3. If the usage exceeds the limit, check the grace period info to make sure that the 14 day GP period has been used.

```
lcmadm get --grace-period-info
```

The system returns an output as the following example:

```
Grace Period Info
Name           Status              Duration(days)    Date Activated   Base l →
imit for GP renewal
FAT1023070     Grace Period Used   14                N/A             100
```

4. Check if the capacity license is already in enforcement:

```
lcmadm get --capacity-enforcement-info
```

if the capacity license is already in enforcement then the system returns an output as the following example:

```
Name           Date Triggered                      Base limit for Enforcemen →
t clearing
FAT1023070     Nov 2 2015 16:00:00 GMT             100
```

Note:

— Refer to Evaluate the License Usage on page 71 to calculate the license usage.

— If the license is in enforcement, need to install a new license at least with 5% capacity increment to base limit for enforcement clearing, and the current usage need to be lower than the new limit.

— As network usage changes, the GP Renew Target and Enforcement Clearing Target changes as well. The limit recorded when GP gets started is used as the base limit for GP renewal and the base limit for enforcement clearing.

— When installing a new capacity license to renew GP or clear enforcement, the latest GP renew target or enforcement clearing target will need to be verified. The commands `lcmadm get -gpi` and `lcmadm get -cei` has to be used to find the base limit for GP renewal and the base limit for enforcement clearing. The base limit is not the renew target and users must calculate the renew target by using the algorithm which is described in network impact.

— Other Network Pack RTC license enforcement has the same troubleshooting step as the Network Packs described in this section.

Results

The node is added to the ENM without errors.

7.1.2 "Error 12001 : Insufficient access rights to perform the operation" Error Message

An insufficient access privilege issue occurs if the user does not have LCM administrator privilege.

Steps

Verify that the user has one of the following user roles:

— ADMINISTRATOR

— LCM_Administrator

Results

User has the LCM administrator privilege.

7.1.3 "Error 12009 : Command Syntax Error, unrecognized or invalid option <option-name>" Error Message

A LCM command syntax error issue occurs if the command entered does not conform to the defined CLI syntax.

Steps

Refer to *License Control Monitor Administration Tasks* in the ENM System Administration Guide or *CLI Online Help* for the correct syntax to use for the LCM command.

7.1.4 "Error 12117 : Feature: <some_capacity_license_file.txt>, Caused by: Invalid license format>" Error Message

A licence file installation issue occurs if the relevant license file is corrupted.

Steps

Contact appropriate Ericsson organization for a new license file.

Results

The new license file is issued without errors.

7.1.5 Error 12122: Failed to Create License Threshold Data

A license file partial installation issue occurs if the License Threshold data fails to be created.

The license will be installed but some issues may arise.

Steps

Contact the customer support for help.

Note: There is a workaround for this issue, follow the below steps:

1. Remove the license:

   ```
   lcmadm remove name=<LICENSE_NAME>
   ```

2. Install the license again:

   ```
   lcmadm install file: <LICENSE_FILE>
   ```

This will try to create the License Threshold data again.

7.1.6 Error 12123: Failed to Create License Properties Data

A license file partial installation issue occurs if the License Properties data fails to be created.

The license will be installed but some issues may arise.

Steps

Contact the customer support for help.

Note: There is a workaround for this issue, follow the below steps:

1. Remove the license:

   ```
   lcmadm remove name=<LICENSE_NAME>
   ```

2. Install the license again:

   ```
   lcmadm install file: <LICENSE_FILE>
   ```

This will try to create the License Properties data again.

7.1.7 CLI Menu Option is Unavailable

The CLI menu option is not available if a user attempts to logon to the ENM Launcher without CLI access privileges.

Steps

1. Verify that the user has one of the following user roles:
   - ADMINISTRATOR
   - LCM_Administrator
2. Logon to ENM as ADMINISTRATOR and add the appropriate user role for the user.

Results

CLI menu option is available for the user.

7.1.8 Evaluate the License Usage

To perform a licence enforcement the license usage has to be evaluated.

Steps

1. Check the usage of license file already installed on the system:

   ```
   lcmadm list --current-usage
   ```

   If there is at least a installed license file currently in use then the system returns an output as the following example:

   ```
   Name         Expiry Date                 Limit Usage       Usage Recorded     →
      Vendor Info
   FAT1023070   Feb 28 2016 23:59:59 GMT    100   110         Nov 3 2015 16:00:  →
   00 GMT          Radio_Network_Base_Package_numberOf_5MHzSC
   ```

2. To check how the LCM calculate usage per license, open the *Log Viewer* page in ENM GUI and search for the following strings:

Number of 5MHz Sector carrier for the Node {Node FDN} = {Counter}
The total Number of 5MHz Sector carrier in the system = {Total Usage}

Number of KSAU for the Node {Node FDN} = {Counter}
The total Number of KSAU in the system = {Total Usage}

Number of Mgw-SSC for the Node {Node FDN} = {Counter}
The total Number of Mgw-SSC in the system ={Counter}

Results

User retrieves the license usage value.

7.1.9 Perform an Emergency Unlock

This LCM command allows an ENM system administrator to activate the system emergency unlock. The Emergency Unlock feature is available by default.

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.

Enter the following command to activate the ENM system emergency unlock:

```
lcmadm activate (--emergency-unlock | -eu)
```

Steps

1. Activate the emergency unlock.

   ```
   lcmadm activate --emergency-unlock
   ```

   The system returns the following output:

   Example Emergency Unlock Output

   ```
   Emergency unlock successfully activated
   ```

2. Check the emergency unlock activated time, duration, and usage.

   ```
   lcmadm get -eui
   ```

   The system returns the following output:

   Example Emergency Unlock Information Output

   ```
   Emergency Unlock Info Allowed Activation Limit Usage Status
   Duration (days) Date Activated 2 1 Active 7 Nov 09 2016
   13:19:33 GMT
   ```

Results

User performs an emergency unlock.

7.1.10 License Usage Algorithm Description

This section describe how the Capacity License plugins calculate the license usage for the following cases:

7.1.10.1 License Usage Calculation for #5MHZ Sector Carriers

> This section describe how the Capacity License plugins calculate the license usage for the LTE Network 16A Radio Network Base Package: Price parameter #5MHz Sector Carrier.

The Radio_Network_Base_Package_numberOf_5MHzSC maps to NE Type ERBS and RadioNode in ENM 16A/16B. LCM implements a capacity license plugin to support #5 MHz Sector Carriers price parameter.

NE type MSRBS_V1 is added in ENM 17A.

Prerequisites

- New eNodeBs can only be added into ENM is the following requisites are satisfied:
  - A valid #5MHz Cell Carriers capacity license exists and the usage is less than or equal to the capacity license limit (indirect enforcement).
  - The #5MHZ Sector Carrier capacity license Grace Period status is In Grace Period, even if the usage exceeds the limit.
  - After a Grace Period has ended if the usage is lower than or equal to the limit and the usage remains lower than limit.
  - If the #5MHZ Sector Carrier capacity license is removed or expired during the Grace Period, eNodeB can be added for the remaining GP duration.
- New eNodeBs can not be added into ENM if the following conditions occur:
  - The usage of #5MHZ sector carrier exceeds the capacity limits and the Emergency Unlock is not active.
  - The #5MHZ sector carrier license is expired or removed and the Grace Period or Emergency Unlock is not applicable.
  - The usage of the #5MHZ sector carrier exceeds the capacity limits and the Grace Period is used.
- Enforcement is triggered if usage is higher than limit while GP ends. Adding eNodeB is not allowed as enforcement is triggered, deleting eNodeB to lower usage than limit doesn't allow adding new node again. Users have to clear enforcement to be able to add ERBS or RadioNode again.

— The following table lists the prerequisite environment:

Measured Data Source	Number of #5MHz Sector Carriers in DPS
Periodicity	60 minutes
Grace Period Allowed	True (default duration is 14 days)
G.P. Renew Target	Capacity limit increased (>= 5%) and usage is below new limit (usage < limit) (see Note-1 and Note-2)
Enforcement Policy	Block adding of new eNodeB nodes
Enforcement Clearing Target	Capacity limit increased (>= 5%) and usage is below new limit (usage < limit) (see Note-1 and Note-2)

Steps

1. Calculate the required number of 5 MHz sector carrier units for one cell by using the following algorithm:

$$Required\ \ Units = Ceiling\left[\frac{Configured\ Channel\ Bandwidth}{5\ MHz}\right] * No.\ of\ Sector\ Carriers\ of\ the\ Cell$$

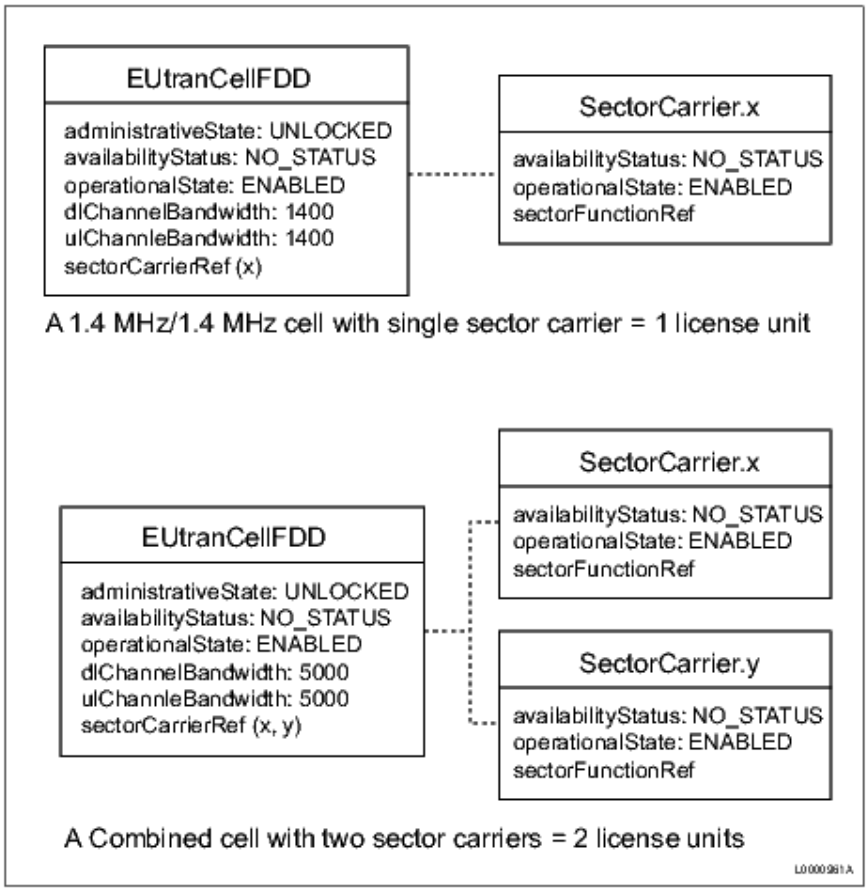
   The algorithm pertains to a 5MHz SC feature *CPI (213/1553-HSC 105 50/1-V1 Uen A) FDD*.

   a. The Channel bandwidth of the cell (FDD or TDD) is available in EUtranCellFDD or EUtranCellTDD MO.

   b. The 5 MHz sector carrier is the capacity granularity per cell per Radio Access Technology (RAT) per node.

   c. The Configured Channel Bandwidth is determined by the higher value of the `dlChannelBandwidth` and the `ulChannelBandwidth` attribute (see Note-3).

   d. The number of sector carriers of a cell is determined by attribute `SectorCarrier`. For example, a 1.4 MHz/3 MHz cell with single sector carrier requires one 5 MHz unit. A 5 MHz cell with two sector carriers requires two units, as shown in the following figure:



e. The following table lists the counters associated with the 5 MHz Sector Carrier feature.

Counter	Description
pmLic5MHzSectorCarrierActual	This counter shows the current amount of allocated capacity licensed 5 MHz sector carriers in the node. The use of 5 MHz sector carriers is monitored and a sample is taken at the end of each Result Output Period (ROP).

f. For nodes that have attribute pmLic5MhzSectorCarrierActual (in class EnodeBFunction). This attribute is a counter and is applicable to the following:

   i. Macro & Micro eNodeBs (CPP based) – 14B and later

g. For nodes that have no attribute pmLic5MhzSectorCarrierActual, but do have SectorCarrier MOs, the algorithm is used and applies to the following:

   i. Macro & Micro eNodeBs (CPP based) – 13A/13B/14A

   ii. G2 eNodeBs (RadioNode)

h. For nodes that have no attribute pmLic5MhzSectorCarrierActual and no SectorCarrier MOs, the algorithm is used and applies to the following (see Note-4).

   i. Macro & Micro eNodeBs (CPP based) – 12B and earlier

   ii. Pico eNodeBs

i. The values for `ulChannelBandwidth` and `dlChannelBandwidth` are:

   i. `1400` kHz

   ii. `3000` kHz

   iii. `5000` kHz

   iv. `10000` kHz

   v. `15000` kHz

   vi. `20000` kHz

Note:

a. The network usage, the GP Renew Target, and Enforcement Clearing Target can change The limit recorded when GP gets started is used as the base limit for GP renewal and the base limit for enforcement clearing.

b. When installing a new capacity license to renew GP or clear enforcement, the latest GP Renew target or Enforcement Clearing Target needs to be verified. The commands `lcmadm get -gpi` and `lcmadm get -cei` are used to find the base limit for GP renewal and the base limit for enforcement clearing. The base limit is not the renew target and users must calculate the renew target using the algorithm.

c. For FDD, it represents the higher of the dl and ul values; and for TDD, it represents the channel bandwidth.

d. For the purpose of the algorithm, 1 cell == 1 sector carrier.

Results

The user can calculate the required number of 5 MHz sector carrier units for one cell.

7.1.10.2 License Usage Calculation for #KSAU Sector Carriers

This section describe how the Capacity License plugins calculate the license usage for the Core Network Base Package (SGSN-MME): Price parameter #KSAU Sector Carrier.

The Core_Network_Base_Package_numberOf_kSAU maps to NE Type SGSN-MME in ENM 16A/16B. LCM implements a capacity license plugin to support #KSAU price parameter.

Prerequisites

- New SGSN-MME can only be added into ENM is the following requisites are satisfied:
  - A valid #KSAU license exists and the usage is less than or equal to the license limit (indirect enforcement).
  - The #KSAU license Grace Period status is In Grace Period, even if the usage exceeds the limit.
  - When a Grace Period has ended if the usage is lower than or equal to the limit and the usage remains lower than limit.
  - If the #KSAU license is removed or expired during the Grace Period, the SGSN-MME can be added for the remaining GP duration.
- New SGSN-MME can not be added into ENM if the following conditions occur:
  - The usage of the #KSAU license exceeds the capacity limits and the Emergency Unlock is not active.
  - The #KSAU license is expired or removed from the system and the Grace Period or Emergency Unlock are not applicable.
  - The usage of the #KSAU license exceeds the capacity limits and the Grace Period is used.
  - Enforcement is triggered if usage is higher than limit while GP ends. Adding SGSN-MME is not allowed as enforcement is triggered, deleting SGSN-MME to lower usage than limit doesn't allow adding new node again. Users have to clear enforcement to be able to add SGSN-MME again.
  - The following table lists the prerequisite environment:

Measured Data Source	**attributes nbrActAttachedSubG, nbrActAttachedSubW, nbrActAttachedSubL in DPS**
Periodicity	60 minutes
Grace Period Allowed	True (default duration is 14 days)
G.P. Renew Target	Capacity limit increased (>= 5%) and usage is below new limit (usage < limit) (See Note-1 and Note-2)
Enforcement Policy	Block adding of new SGSN-MME nodes
Enforcement Clearing Target	Capacity limit increased (>= 5%) and usage is below new limit (usage < limit) (See Note-1 and Note-2)

Steps

1. Per node, get peak measurements over 24 hours.
    a. Every hour, read the 3 attributes from a node.
    b. Sum the three attributes to get a SAU measurement for that node.
2. For each node, calculate its peak (find the largest of its last 24 measurements)
3. Calculate the SAU Usage value:

```
SAU Usage = ? node peak values
```

4. Calculate the KSAU Usage value:

```
KSAU Usage = SAU Usage / 1000
```

For example, If the SAU usage is between 13000 and 13999, the KSAU Usage values is rounded to 13.

Note:
a. The network usage, the GP Renew Target, and Enforcement Clearing Target can change The limit recorded when GP gets started is used as the base limit for GP renewal and the base limit for enforcement clearing
b. When installing a new capacity license to renew GP or clear enforcement, the latest GP Renew target or Enforcement Clearing Target needs to be verified. The commands `lcmadm get -gpi` and `lcmadm get -cei` are used to find the base limit for GP renewal and the base limit for enforcement clearing. The base limit is not the renew target and users must calculate the renew target using the algorithm.

Results

The user can calculate the required number for #KSAU sector carrier.

7.1.10.3 License Usage Calculation for #SCC Sector Carriers

> This section describe how the Capacity License plugins calculate the license usage for the Core Network Base Package (MGW): Price parameter #SCC Sector Carrier.

The Core_Network_Base_Package_numberOf_SCC maps to NE Type MGW in ENM 16B. LCM implements a capacity license plugin to support #SCC price parameter.

Prerequisites

- New MGW can only be added into ENM is the following requisites are satisfied:
  - A valid #SCC license exists and the usage is less than or equal to the license limit (indirect enforcement).
  - The #SCC license Grace Period status is In Grace Period, even if the usage exceeds the limit.
  - When a Grace Period has ended if the usage is lower than or equal to the limit and the usage remains lower than limit.
  - If the #SCC license is removed or expired during the Grace Period, the MGW can be added for the remaining GP duration.
- New MGW can not be added into ENM if the following conditions occur:
  - The usage of the #SCC license exceeds the capacity limits and the Emergency Unlock is not active.
  - The #SCC license is expired or removed from the system and the Grace Period or Emergency Unlock are not applicable.
  - The usage of the #SCC license exceeds the capacity limits and the Grace Period is used.
  - Enforcement is triggered if usage is higher than limit while GP ends. Adding MGW is not allowed as enforcement is triggered, deleting MGW to lower usage than limit doesn't allow adding new node again. Users have to clear enforcement to be able to add MGW again.
  - The following table lists the prerequisite environment:

Measured Data Source	**SCC = pmNrOfMediaStreamChannelsBusy/2.005 Counter pmNrOfMediaStreamChannelsBusy is an attribute of MO MgwApplication in DPS**
Periodicity	60 minutes
Grace Period Allowed	True (default duration is 14 days)
G.P. Renew Target	Capacity limit increased (>= 5%) and usage is below new limit (usage < limit) (see Note-1 and Note-2)
Enforcement Policy	Block adding of new MGW nodes
Enforcement Clearing Target	Capacity limit increased (>= 5%) and usage is below new limit (usage < limit) (see Note-1 and Note-2)

Steps

1. Per node, get peak measurements over 24 hours.
2. Calculate the SSC Usage value:

```
SCC Usage = ? node peak values
```

Note:

- The network usage, the GP Renew Target, and Enforcement Clearing Target can change The limit recorded when GP gets started is used as the base limit for GP renewal and the base limit for enforcement clearing.
- When installing a new capacity license to renew GP or clear enforcement, the latest GP Renew target or Enforcement Clearing Target needs to be verified. The commands `lcmadm get -gpi` and `lcmadm get -cei` are used to find the base limit for GP renewal and the base limit for enforcement clearing. The base limit is not the renew target and users must calculate the renew target using the algorithm.

Results

The user can calculate the required number for #SCC sector carrier.

7.1.10.4 License Usage Calculation for `number_of nodes_R6000`

> This section describes how the Capacity License plugins calculate the license usage for the Core Network Base Package (R6000): the price parameter `number_of_nodes_R6000`.

The Transport_Network_Base_Package_numberOf_Nodes_R6000 license maps to NE Type Router6672, Router6675, Router6x71, Router6273 and Router6274. LCM implements a capacity license plug-in to support the `number_of nodes_R6000` price parameter.

Prerequisites

- New R6000 can only be added into ENM if the following requisites are satisfied:
  - A valid `number_of nodes_R6000` license exists and the usage is less than or equal to the license limit (indirect enforcement).
  - The `number_of nodes_R6000` license Grace Period status is `In Grace Period`, even if the usage exceeds the limit.
  - When a Grace Period has ended if the usage is lower than or equal to the limit and the usage remains lower than limit.
  - If the `number_of nodes_R6000` license is removed or expired during the Grace Period, the R6000 can be added for the remaining GP duration.
- New R6000 cannot be added into ENM if the following conditions occur:

— The usage of the number_of nodes_R6000 license exceeds the capacity limits and the Emergency Unlock is not active.

— The number_of nodes_R6000 license is expired or removed from the system and the Grace Period or Emergency Unlock are not applicable.

— The usage of the number_of nodes_R6000 license exceeds the capacity limits and the Grace Period is used.

— Enforcement is triggered if usage is higher than limit while GP ends. Adding R6000 is not allowed as enforcement is triggered, deleting R6000 to lower usage than limit does not allow adding new node again. Users have to clear enforcement to be able to add R6000 again.

— The following table lists the prerequisite environment:

Measured Data Source	Number of Router6672_Nodes, Router6675_Nodes, Router6x71_Nodes, Router6273_Nodes and Router6274_Nodes NetworkElement MO in DPS
Periodicity	15 minutes
Grace Period Allowed	True (default duration is 14 days)
G.P. Renew Target	Capacity limit increased (>= 5%) and usage is below new limit (usage < limit) (see Note-1 and Note-2)
Enforcement Policy	Block adding of new R6000 nodes
Enforcement Clearing Target	Capacity limit increased (>= 5%) and usage is below new limit (usage < limit) (see Note-1 and Note-2)

Steps

Sum of number of Router6672_Nodes, Router6675_Nodes, Router6x71_Nodes, Router6273_Nodes, and Router6274_Nodes NetworkElement MO in DPS.

Note:

1. The network usage, the GP Renew Target, and Enforcement Clearing Target can change The limit recorded when GP gets started is used as the base limit for GP renewal and the base limit for enforcement clearing.

2. When installing a new capacity license to renew GP or clear enforcement, the latest GP Renew target or Enforcement Clearing Target needs to be verified. The commands `lcmadm get -gpi`and `lcmadm get -cei`are used to find the base limit for GP renewal and the base limit for enforcement clearing. The base limit is not the renew target and users must calculate the renew target using the algorithm.

Results

The user can calculate the required number_of nodes_R6000.

7.1.10.5 License Usage Calculation for number_of nodes_Fronthaul6080

> This section describes how the Capacity License plugins calculate the license usage for the Transport Network Base Package (Fronthaul 6080): the price parameter is the number_of_nodes_Fronthaul.

The Transport_Network_Base_Package_numberOf_Nodes_Frontahaul license maps to the NE Type FRONTHAUL-6080. LCM implements a capacity license plugin to support the number_of nodes_Fronthaul price parameter.

Prerequisites

- New Fronthaul 6080 can only be added into ENM if the following requisites are satisfied:
  - A valid number_of nodes_Fronthaul license exists and the usage is less than or equal to the license limit (indirect enforcement).
  - The number_of nodes_Fronthaul license Grace Period status is In Grace Period, even if the usage exceeds the limit.
  - When a Grace Period has ended if the usage is lower than or equal to the limit and the usage remains lower than limit.
  - If the number_of nodes_Fronthaul license is removed or expired during the Grace Period, the Fronthaul 6080 can be added for the remaining GP duration.
- New Fronthaul 6080 can not be added into ENM if the following conditions occur:
  - The usage of the number_of nodes_Fronthaul license exceeds the capacity limits and the Emergency Unlock is not active.
  - The number_of nodes_Frontahaul license is expired or removed from the system and the Grace Period or Emergency Unlock are not applicable.
  - The usage of the number_of nodes_Fronthaul license exceeds the capacity limits and the Grace Period is used.
  - Enforcement is triggered if usage is higher than limit while GP ends. Adding Fronthaul 6080 is not allowed as enforcement is triggered, deleting Fronthaul 6080 to lower usage than limit doesn't allow adding new node again. Users have to clear enforcement to be able to add Fronthaul 6080 again.
  - The following table lists the prerequisite environment:

Measured Data Source	number of Fronthaul 6080_Nodes NetworkElement MO in DPS
Periodicity	15 minutes

Measured Data Source	number of Fronthaul 6080_Nodes NetworkElement MO in DPS
Grace Period Allowed	True (default duration is 14 days)
G.P. Renew Target	Capacity limit increased (>= 5%) and usage is below new limit (usage < limit) (see Note-1 and Note-2)
Enforcement Policy	Block adding of new Fronthaul 6080 nodes
Enforcement Clearing Target	Capacity limit increased (>= 5%) and usage is below new limit (usage < limit) (see Note-1 and Note-2)

Steps

Sum of number of Fronthaul 6080_Nodes NetworkElement MO in DPS.

Note:

1. The network usage, the GP Renew Target, and Enforcement Clearing Target can change The limit recorded when GP gets started is used as the base limit for GP renewal and the base limit for enforcement clearing.

2. When installing a new capacity license to renew GP or clear enforcement, the latest GP Renew target or Enforcement Clearing Target needs to be verified. The commands `lcmadm get -gpi` and `lcmadm get -cei` are used to find the base limit for GP renewal and the base limit for enforcement clearing. The base limit is not the renew target and users must calculate the renew target using the algorithm.

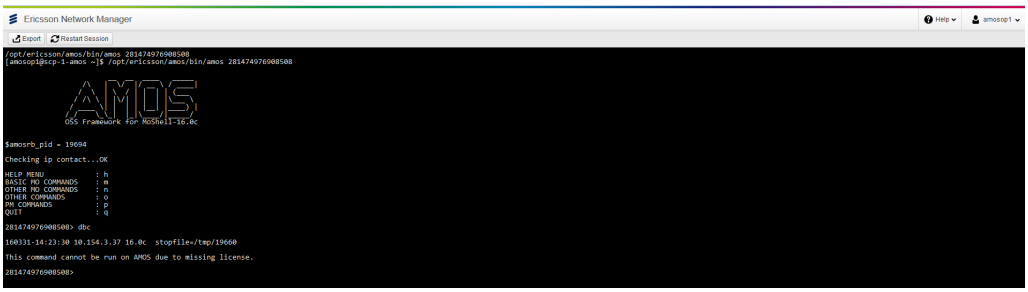
Results

The user can calculate the required number_of nodes_Fronthaul.

7.1.11 Troubleshooting Polyview License

This section describes how to troubleshoot the following Polyview issue:

Error: This command cannot be run on AMOS due to missing license



Prerequisites

You must have Amos_Operator or Amos_Administrator role. If you do not have an AMOS role, you cannot run the AMOS command

Steps

1. Use command "`lcmadm list`" on ENM Command Line Interface (CLI) to check if the FAT1023472 license is installed.

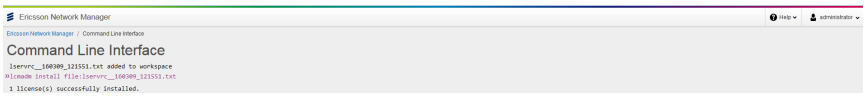
   Under section 'Feature License Info' POLYVIEW license, VP_Advanced_MO_Scripting_NC_onOffScope_LTE_5MHzSC should be displayed.

2. If this is not displayed, do the following steps:

   a. Drag and drop the POLYVIEW license file from Windows Explorer (or file manager) into the ENM CLI

   b. Install the POLYVIEW license through the ENM CLI

```
lcmadm install file: <file name>
```



3. Use the following command to verify POLYVIEW license installation:

   '`lcmadm list`'. This lists the installed licenses.

   POLYVIEW license name "VP_Advanced_MO_Scripting_NC_onOffScope_LTE_5MHzSC" should be displayed under 'Feature License Info'.

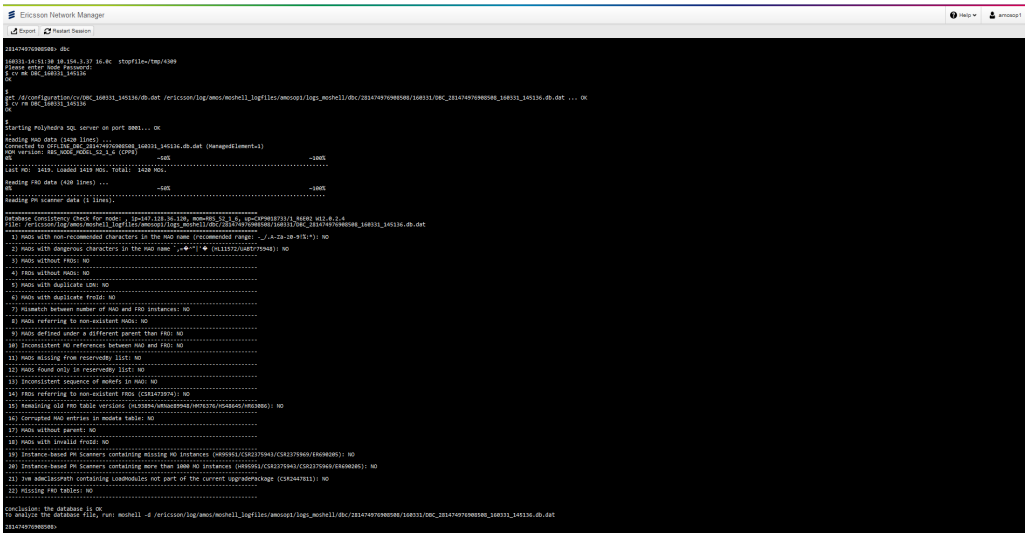
Note: For more details about ENM Licensing, refer to *License Control Monitor Administration Tasks* in the ENM System Administration Guide.

Example

If a valid license of polyview is installed, you can run `'dbc'` command over AMOS.

Results

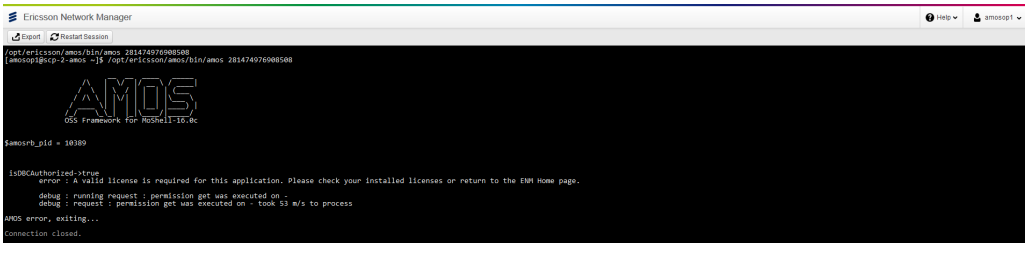
When `'dbc'` command is executed over AMOS it should run OK. The license error will not be displayed when `'dbc'` command is run over AMOS.



7.1.12 Troubleshooting AMOS License

This section describes how to troubleshoot the following AMOS license issue:

Error: A valid license is required for this application. Please check your installed licenses or return to the ENM Home page



Prerequisites

You must have Amos_Operator or Amos_Administrator role.

Note: If you do not have an AMOS role, you cannot run the AMOS command.

Steps

1. Use the command `'lcmadm list'` on Command Line Interface (CLI) to check if the license (FAT1023078 with Advanced MO Scripting on it) is installed.

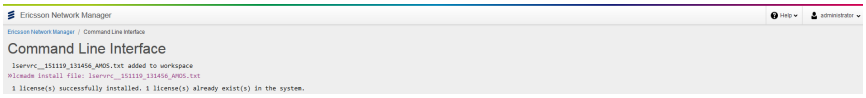
   Under section 'Feature License Info' `AMOS license VP_Advanced_MO_Scripting_onOffScope_LTE_5MHzSC` should display.

2. If not. complete the following steps:

   a. Drag and drop the AMOS license file from Windows Explorer (or file manager) into the CLI.

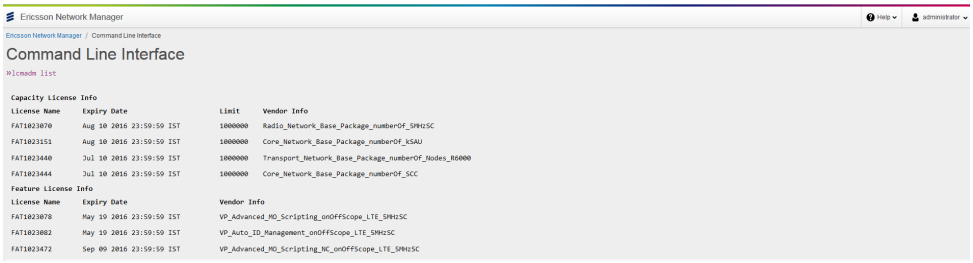
   b. Install the AMOS license through CLI.

```
lcmadm install file: <file name>
```



3. Using the following command, verify AMOS license installation: `'lcmadm list'`.

   This lists the licenses installed:



   AMOS license name `VP_Advanced_MO_Scripting_onOffScope_LTE_5MHzSC` should display under 'Feature License Info'.

Note: For more details about ENM Licensing, refer to *License Control Monitor Administration Tasks* in the ENM System Administration Guide.

Results

The license error is not displayed when AMOS is launched against a node with a valid license installed.

7.2 Troubleshooting SMRS Service

This section provides the troubleshooting steps recommended to diagnose and fix common problems in SMRS.

7.2.1 SMRS Directory Structure

> This section provides the troubleshooting steps recommended to diagnose and fix common problems that can be encountered in SMRS file system directory structure

Prerequisites

`/home/smrs` directory should be present in SMRS file system location.

Steps

1. Check that SMRS home location is present and corresponding account directory created under `/home/smrs/smrsroot/`

   ```
   ls -ltr
   ```

2. Verify `/home/smrs` directory path and account directory are created with appropriate permission, ownership and group ownership.

   file permission : 775

   ownership : jboss_user

   Group ownership : mm-smrsusers

   Example

   ```
   ls -ltr

   drwxrwsr-x+ 13 jboss_user mm-smrsusers 1024 Apr 29 03:11 software
   drwxrwsr-x+ 13 jboss_user mm-smrsusers 1024 Apr 29 03:11 backup
   drwxrwsr-x+ 13 jboss_user mm-smrsusers 1024 Apr 29 03:11 licence
   ```

7.2.2 SMRS File System Mount Point

> This section provides the troubleshooting steps recommended to diagnose and fix common problems that can be encountered in SMRS file system mount point.

Prerequisites

— SMRS mount point is mounted and storage memory is allocated.

Mount point path : `/ericsson/tor/smrs`

— `/ericsson/tor/smrs` should bind with `/home/smrs`

Steps

1. If mounted file system is not found for SMRS, verify using:

```
df -ah /home/smrs
```

This command gives mount point and memory allocation details for the SMRS file system. It is mounted to `/ericsson/tor/smrs`

Example

```
Filesystem          Size  Used Avail Use% Mounted on
/ericsson/tor/smrs   10G  514M  9.0G   6% /home/smrs
```

Results

7.2.3 Failure During SFTP Connections

This section provides the troubleshooting steps recommended to diagnose and fix common problems that can be encountered in SMRS to open SFTP connections by nodes. SFTP connection can be failed with error message "FTP server is not accessible".

7.2.3.1 Check if sshd Service is Running on smrsserv VM

Check if sshd Service is Running on smrsserv VM

Prerequisites

A command window must be opened and you need to have the system administrator privileges on smrsserv VM.

Steps

1. Perform the steps in Connect to a Service on page 2 and log on to the smrsserv Virtual Machines on SVC nodes.
2. Check if sshd service is running:

```
[root@svc-1-smrsserv cloud-user]# service sshd status
openssh-daemon (pid  <xxxx>) is running...
```

   If sshd service is not running, restart the sshd service.

3. If service sshd is not running on any of smrsserv VMs, start the service:

```
[root@svc-1-smrsserv cloud-user]# service sshd start
openssh-daemon (pid  <xxxx>) is running...
```

7.2.3.2 Check if SMRS Users is Correctly Created in OpenDJ and nslcd Service Running

Check if SMRS users have been correctly created in opendj and nslcd service running

Prerequisites

A command window must be opened and you need to have the system administrator privileges on smrsserv VM.

Steps

1. Perform the steps in Connect to a Service on page 2 and log on to the smrsserv Virtual Machines on SVC nodes.
2. Check if nslcd service is running:

```
[root@svc-1-smrsserv cloud-user]# service nslcd status
nslcd (pid  <xxxx>) is running...
```

   If nslcd service is not running, restart the nslcd service.

```
[root@svc-1-smrsserv cloud-user]# service nslcd start
```

3. Check if expected users and group have been correctly created in openDJ. Expected group id is 5000.

```
[root@svc-1-smrsserv cloud-user]# getent passwd |grep mm-*

mm-ul_spectrum_files:*:20000:5000::/home/smrs/smrsroot/ul_spectrum_files/:/s →
bin/nologin
```

```
mm-licence:*:20001:5000::/home/smrs/smrsroot/licence/:/sbin/nologin
mm-backup:*:20002:5000::/home/smrs/smrsroot/backup/erbs/:/sbin/nologin
mm-mli-backup:*:20003:5000::/home/smrs/MINI-LINK/MINI-LINK-Indoor/tn_backup_ →
configuration/:/sbin/nologin
mm-software:*:20004:5000::/home/smrs/smrsroot/software/erbs/:/sbin/nologin

[root@svc-1-smrsserv cloud-user]#  getent group | grep mm-smrs*
mm-smrsusers:x:5000:jboss_user
mm-smrsusers:*:5000:mm-backup,mm-licence,mm-software,mm-mli-backup
```

4. If no nslcd service is running after restart, the nslcd service and the group id is not 5000 for mm-* user, contact Ericsson support for further assistance.

7.2.3.3 Check if SFTP Client (Network Element) has enabled the Secure File Transfer Protocol

Check if SFTP Client (Network Element) has enabled the Secure File Transfer Protocol

Prerequisites

A command window must be opened and you need to have the system administrator privileges on smrsserv VM.

Steps

1. Open an AMOS session towards the node

```
amos <node_ipaddress>
```

2. Check whether the SFTP client (node) has enabled the Secure File Transfer Protocol (SFTP).

   Verify in the resulting output: FileXferClient secure, node internal file transfer client uses SFTP.

```
secmode -s

Security configuration settings:
Access method Current security mode
-------------------------------------------------------------
TelnetFtpServers
unsecure, node internal Telnet and FTP servers are ON.
TargetMonitor
secure, node Target Monitor is OFF
DbgServerUdpLnh secure, Debug server and UDP Linkhandler are OFF.
FileXferClient secure, node internal file transfer client uses SFTP.
CorbaSecurity unsecure, corba security is OFF.
OperationalSecLevel level 1
ConfiguredSecLevel level 1
```

```
[root@svc-1-smrsserv
```

3. If FileXferClient is unsecure, enable SFTP on networkElement.

7.2.3.4 Check if SMRS Directory Structure and File Permissions are Correct

Check if SMRS Directory Structure and File Permissions are Correct

Prerequisites

A command window must be opened and you need to have the system administrator privileges on smrsserv VM.

Steps

1. Perform the steps in Connect to a Service on page 2 section and log on to the smrsserv Virtual Machines on SVC nodes.
2. Check for smrs home location should be present and corresponding account directory created under `/home/smrs/` and `/home/smrs/smrsroot/`

   ```
   [root@svc-1-smrsserv cloud-user]# ls -ltr /home/smrs/
   [root@svc-1-smrsserv cloud-user]# ls -ltr /home/smrs/smrsroot/
   ```

   Verify if `/home/smrs` directory path and account directory are created with appropriate file permission, ownership and group ownership. The file permission, ownership, group ownership should correspond to:

   ```
   file permission : 775(Owner and Group permission: Read, Write
   , Execute)
   ownership : jboss_user
   Group ownership : mm-smrsusers
   ```

   Sample Output:

   ```
   [root@svc-1-smrsserv cloud-user]# ls -ltr /home/smrs/
   drwxrwsr-x+ 11 jboss_user mm-smrsusers 4096 Sep 21 12:58 smrs
   root

   [root@svc-1-smrsserv cloud-user]# ls -ltr /home/smrs/smrsroot
   /
   drwxrwsr-x+ 13 jboss_user mm-smrsusers 1024 Apr 29 03:11 soft
   ware
   drwxrwsr-x+ 13 jboss_user mm-smrsusers 1024 Apr 29 03:11 back
   up
   drwxrwsr-x+ 13 jboss_user mm-smrsusers 1024 Apr 29 03:11 lice
   nce
   ```

3. If directory permissions are not as expected, contact local Ericsson support.

7.2.3.5 Check if SMRS Filesystem Mount Point Bind Mounted Correctly

Check if SMRS Filesystem Mount Point Bind Mounted Correctly

Prerequisites

A command window must be opened and you need to have the system administrator privileges on smrsserv VM.

Steps

1. Perform the steps in Connect to a Service on page 2 and log on to the smrsserv Virtual Machines on SVC nodes.
2. Check the smrs filesystem bind mounted correctly. Filesystem :/ `ericsson/tor/smrs`, Mounted on: /home/smrs/

   ```
   df -ah /home/smrs
   ```

   This command gives mount point and memory allocation details for SMRS file system. It should be mounted to `/ericsson/tor/smrs`

   Sample Output:

   ```
   Filesystem          Size  Used Avail Use% Mounted on
   /ericsson/tor/smrs   10G  514M  9.0G   6% /home/smrs
   ```

3. If `/home/smrs` filesystem not mounted to `/ericsson/tor/smrs/`, contact local Ericsson support.

7.2.3.5.1 Failure during SMRS Housekeeping for Accounts

This section provides the troubleshooting steps recommended to diagnose and fix common problems that can be encountered in SMRS housekeeping for accounts.

7.2.3.5.1.1 Check the SMRS Housekeeping Retention Policy

Check the SMRS housekeeping retention policy for the account and check all latest files available on SMRS filesystem based on housekeeping retention policy.

Prerequisites

A command window must be opened and you need to have the system administrator privileges on smrsserv VM.

Steps

1. Perform the steps in Configuring PIB Parameters on page 8 and read or update the retention policy of SMRS housekeeping
2. Perform the steps in Connect to a Service on page 2 section and log on to the smrsserv Virtual Machines on SVC nodes.
3. Check the number of files available in the SMRS filesystem for Backup account. Available backup files should be equal to retention policy and all available files should have latest timestamp. Older files are only deleted by SMRS housekeeping.

```
[root@svc-1-smrsserv cloud-user]# ls -ltr /home/smrs/smrsroot/backup/<nodeType> →
/<NodeName>/

Example:
[root@ieatenmpd102-smrsserv-0 cloud-user]# ls -ltr /home/smrs/smrsroot/backup/e →
rbs/ieatnetsimv6070-25_LTE26ERBS00071
total 24
-rw-rw-r--+ 1 mm-backup mm-smrsusers 4061 Sep 24 12:57 VThk8w.zip
-rw-rw-r--+ 1 mm-backup mm-smrsusers 4059 Sep 25 12:57 sgkJBF.zip
-rw-rw-r--+ 1 mm-backup mm-smrsusers 4061 Sep 26 12:57 bjzid4.zip
```

4. If number of Backup files exceeds retention policy, trigger SMRS housekeeping, refer to the ENM System Administration Guide.
5. If number of backup files still exceeds retention policy, contact local Ericsson support.

   Note: The number of backups may vary based on time when the SMRS filesystem was verified. Automatic default start time of housekeeping is 3:00AM

7.2.3.5.1.2 Check the Space Usage of SMRS Filesystem has not Exceeded 80%

Check that the space usage of the SMRS filesystem has not exceeded 80%

Prerequisites

A command window must be opened and you need to have the system administrator privileges on smrsserv VM.

Steps

1. Perform the steps in Configuring PIB Parameters on page 8 and read or update the used space threshold `usedStorageThresholdForSMRS` of SMRS housekeeping

Default value of parameter `usedStorageThresholdForSMRS` is 80.

2. Perform the steps in Connect to a Service on page 2 section and log on to the smrsserv Virtual Machines on SVC nodes.
3. Check the used space of SMRS filesystem. % used should not exceed 80% (default) or configured values after SMRS housekeeping.

```
df -ah /home/smrsv
```

This command displays used space of smrs filesystem:

```
Filesystem          Size  Used Avail Use% Mounted on
/ericsson/tor/smrs   10G  514M  9.0G   6% /home/smrs
```

4. If SMRS filesystem used space exceeds 80%(default) or configured value, trigger SMRS housekeeping, refer to the ENM System Administration Guide.
5. If used space remains at more than 80% or number of backup files more than retention policy, contact local Ericsson support.

7.3 Troubleshooting HTTPD

7.3.1 Connection Errors in HTTPD Access Logs

> This topic describes how to troubleshoot "Connection was aborted" errors associated with ENM web services.

Prerequisites

— Access to the Management Server (MS) and Peer Nodes.

— Basic knowledge of Linux and Networking.

The exception: `java.lang.IllegalStateException: Connection was aborted` is displayed in `/var/log/messages` of `httpd` VM logs.

Steps

1. Collect the `/var/log/messages` logs from `httpd` VM.
    a. Log on to the ENM MS as the **`litp-admin`** user and switch to the **`root`** user.

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

```
# ssh litp-admin@<MangementServer>
# su -
```

b. Log on to `httpd` VM as `cloud-user`

```
# ssh -i /root/.ssh/vm_private_key cloud-user@<svc-*-h
ttpd>
```

c. Open messages log file

```
# cd /var/log/
```

```
# cat messages
```

d. Check for the `java.lang.IllegalStateException: Connection was aborted` exception.

Note: In `/ericsson/3pp/haproxy/data/config/haproxy-ext.cfg` file of haproxy, both `"timeout http-keep-alive"` and `"timeout http-request"` properties values are, by default, set to 10 seconds.

Example

```
> ssh root@ieatlms6357
############  WARNING  #############

This system is for authorised use only. By using this system you co
nsent to monitoring and data collection.

###################################
root@ieatlms6357's password:
Last login: Thu Aug 10 07:27:00 2017 from atrcts6.athtem.eei.ericss
on.se
[07:27:43 root@ieatlms6357:~ ]# bash
[07:27:45 root@ieatlms6357:~ ]# ssh litp-admin@haproxy
Warning: Permanently added 'haproxy' (RSA) to the list of known hos
ts.
############  WARNING  #############

This system is for authorised use only. By using this system you co
nsent to monitoring and data collection.

###################################
Last login: Wed Aug  9 13:38:13 2017 from ieatlms6357
[litp-admin@ieatrcxb6449 ~]$ su
Password:
[root@ieatrcxb6449 litp-admin]# cd /ericsson/3pp/haproxy/data/confi
g/
[root@ieatrcxb6449 config]# less haproxy-ext.cfg | grep 'timeout ht
tp'
    timeout http-request    10s
    timeout http-keep-alive 10s
    option http-server-close
```

```
[root@ieatrcxb6449 config]#
```

2. Check below link for more details on "timeout http-keep-alive" and "timeout http-request" properties.

   https://cbonte.github.io/haproxy-dconv/configuration-1.5.html#timeout%20http-keep-alive

   This redefines the connection to persist for 10 seconds regardless of the value defined for "KeepAliveTimeout" in the config file in the HTTPD VM, despite the value (KeepAliveTimeout 15) defined in the /etc/httpd/httpd.conf file of HTTPD VM. When a connection expires after 10 seconds, no error is returned from haproxy, but the connection closes.

   Meanwhile, In haproxy, the property "option http-server-close" in the /ericsson/3pp/haproxy/data/config/haproxy-ext.cfg file retains the session on the client side but closes the session on the server side. So, it is an expected behavior.

   It is recommended to use a polling interval of less than 10 seconds in the script in order to avoid this HTTP persistent connection aborted error.

7.3.2 Gateway Timeout Errors in HTTPD Access Logs

Use this information to troubleshoot "HTTP/1.1" 504 " errors associated with httpd access log.

Timeout and KeepAliveTimeOut directives:

Timeout : Timeout (Timeout value is 120 sec defined in httpd.conf under /etc/httpd/conf/) defines , in seconds, the amount of time that the server waits for receipts and transmissions during communications.

KeepAliveTimeout : KeepAliveTimeout sets the number of seconds (KeepAliveTimeout value is 60 sec defined in 12_balancer.conf under /etc/httpd/conf.d/) the server waits after a request has been served before it closes the connection. Once the server receives a request, the Timeout directive applies instead KeepAliveTimeout.

Prerequisites

Access to the Management Server (MS) and Peer Nodes.

Basic knowledge of Linux and Networking.

Steps

1. Collect the `/var/log/httpd/access.log` from `httpd` VM. Log on to the ENM MS as the **`litp-admin`** user and switch to the **`root`** user.

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

   ```
   # ssh litp-admin@<MangementServer>
   # su -
   ```

2. Log on to `httpd` VM as `cloud-user`

   ```
    # ssh -i /root/.ssh/vm_private_key cloud-user@<svc-*-httpd>
   ```

3. Open access log file:

   ```
   ```

   Check for the "HTTP/1.1" 504" exception: # cd /var/log/httpd # less access_log

   ```
   This system is for authorised use only. By using this system you consent to monitoring and data collection.
   ##################################
   Last login: Fri Nov 10 09:28:44 2017 from ieatlms3841
   [root@ieatlms3841 ~]# ssh root@ms-1
   ############  WARNING  ############
   This system is for authorised use only. By using this system you consent to monitoring and data collection.
   ##################################
   root@ms-1's password:
   Last login: Fri Nov 10 08:33:08 2017 from 172.16.207.66
   [root@ieatlms3841 ~]# ssh -i /root/.ssh/vm_private_key cloud-user@svc-3-httpd
   [cloud-user@svc-3-httpd ~]$ sudo su
   [root@svc-3-httpd cloud-user]# cd /var/log/httpd
   [root@svc-3-httpd log]# less less access_log |grep 'HTTP/1.1" 504'
   Nov  1 09:22:40 svc-4-httpd httpd_access_log: 10.247.246.4 - Administrator [01/Nov/2017:09:22:03 +0000] "GET /managedObjects/search/v2?query=select%20all%20objects%20of%20type%20MeContext%2C%20object%20ManagedElement%2C%20object%20ENodeBFunction%2C%20object%20EUtranCellFDD%2C%20object%20EUtranFreqRelation%20where%20MeContext%20has%20child%20ManagedElement%20and%20ManagedElement%20has%20child%20ENodeBFunction%20and%20ENodeBFunction%20has%20child%20EUtranCellFDD%20and%20EUtranCellFDD%20has%20child%20EUtranFreqRelation&orderby=moName&orderdirection=asc HTTP/1.1" 504 148 "https://ieatenm5438-6.athtem.eei.ericsson.se/" "Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36" 172.16.207.91 networkexplorer
   ```

   When httpd sends a request to an Application Server, the connection is open for 60 sec(As per the `keepAliveTimeOut` directive defined in `12_balancer.conf` under `/etc/httpd/conf.d/`). If server has not received the request, then `httpd` closes the connection and displays `504 error`(Gateway time-out at 1 min) in `/var/log/httpd/access_log`. If server receives the request, then the `Timeout` directive applies instead of `keepAliveTimeout`. If the response is not received within two minutes, the connection is closed(Gateway time-out at two minutes).

7.4 Troubleshooting Node Health Check

The Health Check application is a diagnostic tool to check the state of nodes, and provides an easy way to determine node health status: healthy, not healthy, or warning.

The following table lists error scenarios that may occur while running a Node Health Check (NHC) report. The table also lists the related failure message displayed in the **Report Logs** page. The relevant procedures to troubleshoot and fix these issues are described in the following subsections.

Scenario	Comment
NHC Report Fails with Report Logs Message: "HC job MO creation failed: Cannot perform operation as CM supervision is disabled on the node". on page 99	For the NHC Report to be successful, nodes must be SYNCHRONIZED with ENM.
NHC Report Fails with Report Logs Message: "Node Model information is not available" on page 100	For the NHC Report to be successful, with Predefined health check configuration (Category), Baseband Radio Node should be of L18-Q3 version or above.
Health Check of Node is NOT_HEALTHY on page 101	To see the reason for the node health status, check the **Rule Execution** page on the Node Health Check ENM GUI.
NHC Report Fails with Report Logs Message: "Alarm request retrieval failed marking alarm check has failed. Health Status is "UNDETERMINED" on page 101	For successful NHC report execution with additional health check, FM Alarm Supervision must be active.
Unable to Create eNodeB Baseband Radios Profile When There are no Supported Software Packages in ENM on page 102	Supported software package version has to be imported to ENM for successful profile creation.
Mismatch of the Health Check Rules Count in a NHC Report and the Populated Profile Rules Count on page 102	It is recommended to import (to ENM) and choose current software package version in profile creation.
Report Execution Fails with Reports Log Message "HcJob MO creation failed. Reason: Transaction rolled back" on page 103	It is recommended to import (to ENM) and choose current software package version in profile creation.
Unable to View Rule Execution Details Link in a Report Details Page on page 103	It is displayed once health check report execution is complete.

Scenario	Comment
NHC Report Fails with Report Log Message: "Nodes does not allow rule customization" on page 103	For the NHC Report to be successful with Custom health check configuration (Profile), Baseband Radio Node must be of 20.Q2 version or above.
Mismatch in Undetermined node count of **Health Status** tables under **Overview** tab in **Report summary** for `RadioNode` type.	Selecting a few Unsynchronized Radio nodes for report creation leads to a failed report. Therefore, the health status of the node is undetermined. However, the report is not counted for Undetermined nodes in the **Health Status** table of **Report Summary** under the **Overview** tab. User can verify the report logs by clicking **View Report Logs**.

7.4.1 NHC Report Fails with Report Logs Message: "HC job MO creation failed: Cannot perform operation as CM supervision is disabled on the node".

Steps

1. Check the value of the `CmFunction` syncStatus attribute and the value of the `CmNodeHeartbeatSupervision` active attribute using the ENM CLI :

```
cmedit get NetworkElement=<networkElement>,CmFunction=1
```

Example:

```
cmedit get NetworkElement=LTE06dg2ERBS00001,CmFunction=1
FDN : NetworkElement=LTE06dg2ERBS00001,CmFunction=1
CmFunctionId : 1
failedSyncsCount : 1
iposCopyConfigFrequency : 64800
lastFailedSync : Fri Nov 16 03:11:44 GMT 2018
lostSynchronization : null
syncStatus : UNSYNCHRONIZED

1 instance(s)
```

```
cmedit get NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1
```

Example:

```
cmedit get NetworkElement=LTE06dg2ERBS00001,CmNodeHeartbeatSu →
pervision=1
FDN : NetworkElement=LTE06dg2ERBS00001,CmNodeHeartbeatSupervi →
sion=1
```

```
CmNodeHeartbeatSupervisionId : 1
active : true
heartbeatInterval : 420
heartbeatTimeout : 10
heartbeatTimestamp : 0
numberOfRetries : 3

1 instance(s)
```

Note: The `CmFunction` syncStatus attribute must be SYNCHRONIZED, the `CmNodeHeartbeatSupervision` active attribute must be true.

2. If the `CmFunction` syncStatus is UNSYNCHRONIZED, and `CmNodeHeartbeatSupervision` active is false, change `CmNodeHeartbeatSupervision` active to true:

```
cmedit set NetworkElement=<networkElement>,CmNodeHeartbeatSupervision=1 acti →
ve=true
```

Example:

```
cmedit set NetworkElement=LTE06dg2ERBS00001,CmNodeHeartbeatSupervision=1 act →
ive=true
SUCCESS FDN : NetworkElement=LTE06dg2ERBS00001,CmNodeHeartbeatSupervision=1

1 instance(s) updated
```

Note: It may take a few seconds for the `CmFunction` syncStatus attribute value to change to SYNCHRONIZED. When the node has SYNCHRONIZED, create the NHC Report again.

3. If the `CmFunction` syncStatus attribute remains UNSYNCHRONIZED, perform a manual sync:

```
cmedit action NetworkElement=<networkElement>,CmFunction=1 sync
```

Note: If the `CmFunction` syncStatus attribute value still remains UNSYNCHRONIZED, contact local Ericsson support.

7.4.2 NHC Report Fails with Report Logs Message: "Node Model information is not available"

Steps

1. From the ENM CLI, check if Radio Node version is L18-Q3:

```
cmedit get NetworkElement=<networkElement>
```

2. Check if Node is "CM SYNCHRONIZED":

If node is not "CM SYNCHRONIZED", then enable the `CmNodeHeartbeatSupervision`.

Note: To check node status follow the steps set out in NHC Report Fails with Report Logs Message: "HC job MO creation failed: Cannot perform operation as CM supervision is disabled on the node". on page 99

7.4.3 Health Check of Node is NOT_HEALTHY

Steps

1. Go to the **Node Health Check** page.
2. Select the required report on the **Health Check Reports** page.
3. Click on the **Report** details, on the top-left side.
4. Click on the **Rule Execution** page to see the reason for the node health status.

7.4.4 NHC Report Fails with Report Logs Message: "Alarm request retrieval failed marking alarm check has failed. Health Status is "UNDETERMINED"

If FM alarm supervision is not active, then health check report fails with the following report logs message when it is executed with additional health check options.

```
Alarm request retrieval failed marking alarm check has failed. Health Status is
"UNDETERMINED
```

The active attribute of `FmAlarmSupervision` must be **`true`** for successful report execution.

To check FM alarm supervision `active` attribute, run the following command from ENM Cliapp.

```
»cmedit get NetworkElement=RNC102RBS0001,FmAlarmSupervision=1
FDN : NetworkElement=RNC102RBS0001,FmAlarmSupervision=1
FmAlarmSupervisionId : 1
active : true
automaticSynchronization : true
failoverCount : 0
heartbeatinterval : 100
heartbeatTimeout : 300

1 instance(s)
```

Run the following command from ENM Cliapp to change or set FM alarm supervision `active` attribute to **`true`** when the value is `false`.

```
»cmedit set NetworkElement=RNC102RBS0001,FmAlarmSupervision=1 active=true
SUCCESS FDN : NetworkElement=RNC102RBS0001,FmAlarmSupervision=1

1 instance(s) updated
)
```

7.4.5 Unable to Create eNodeB Baseband Radios Profile When There are no Supported Software Packages in ENM

Profile cannot be created, if the supported software package version is not imported to ENM.

Profile creation is currently supported for eNodeB Baseband Radio nodes and support is from 20.Q1 release onwards. Therefore, relative package must be imported to ENM.

7.4.6 Mismatch of the Health Check Rules Count in a NHC Report and the Populated Profile Rules Count

Mismatch of health check rules count between a Node Health Check (NHC) report and a populated profile rules can happen because of the reasons listed in the following sections.

Health Check Rules in a Profile are More Than on a Node

If a health check report is run with a profile where health check rules are not customized, then these rules are not run as part of the report. Hence, these health check rules are not displayed in the **Rule Execution Details** page on the NHC GUI.

If selected software package version in a profile and the node software version on which executed health check report are not same, mismatch can be observed on the number of rules either at populated profile rules or rules on a node.

Health Check Rules on the Nodes are Not in a Profile but Health Check Report is Run with That Profile

If health check Rules on the Nodes are Not in a Profile but Health Check Report is Run with that Profile, the health check rules get executed as part of the report with its default configurations. Hence, there are more rules displayed on **Rule Execution Details** page on the Node Health Check (NHC) GUI.

If selected software package version in a profile and the node software version on which executed health check report are not same, mismatch can be observed on the number of rules either at populated profile rules or rules on a node.

Customized Health Check Rule

A health check rule that is customized by excluding it from a profile is not run as part of the report. Hence, it is not displayed on the **Rule Execution Details** page on the Node Health Check (NHC) GUI.

Do not customize a health check rule if it has to be part of the report.

Note: It is recommended to import the health check rules (to ENM) and choose current software package version in profile creation.

7.4.7 Report Execution Fails with Reports Log Message "HcJob MO creation failed. Reason: Transaction rolled back"

When a health check rule with a default configuration is modified during the profile creation and if the same health check rule is not present on the node; then report execution itself fails with the following reports log message.

```
"HcJob MO creation failed. Reason: Transaction rolled back"
```

The reason being the rule does not exist on the node.

If selected software package version in a profile and the node software version on which executed health check report are not same, mismatch can be observed on the number of rules either at populated profile rules or rules on a node.

7.4.8 Unable to View Rule Execution Details Link in a Report Details Page

When health check report is in a running state, **Rule Execution Details** link is not displayed.

Once the health check report execution is complete, **Rule Execution Details** is displayed to check detailed rule execution information.

7.4.9 NHC Report Fails with Report Log Message: "Nodes does not allow rule customization"

Run the following steps when NHC report fails with log message, `Nodes does not allow rule customization`.

1. From the ENM CLI, check if Radio Node version is 20.Q2.

   ```
   cmedit get NetworkElement=<networkElement>
   ```

2. Check if node is `CM SYNCHRONIZED`. If node is not `CM SYNCHRONIZED`, enable the **`CmNodeHeartbeatSupervision`**.

To check node status, follow the steps in section NHC Report Fails with Report Logs Message: "HC job MO creation failed: Cannot perform operation as CM supervision is disabled on the node". on page 99

7.4.10 Profile Creation Fails with a Message: "Profile creation failed as maximum limit reached"

The default maximum allowed profile count is 100. You are not allowed to create a profile if the profile count reached the maximum limit. The following error message is displayed.

```
"Profile creation failed as maximum limit reached."
```

To create a new profile, delete any profiles, which are not in use and try again.

7.4.11 Failure During Profile Deletion

NHC provides housekeeping policies to ensure that failed deleted profiles do not cause data storage space issues.

Housekeeping Policies

The housekeeping of the failed deleted profiles runs after 1 hour of VM restart.

7.5 Troubleshooting Element Manager

This section describes how to troubleshoot failures related to Element Manager.

7.5.1 Fronthaul 6020 WebUI Autologin Browser Certificate Exemption

Diagnostics

When the user launches the **Element Manager** web UI/LCT for Fronthaul 6020 node, following are the cases where a certification exception is observed in the remote desktop browser.

— LCT launched for the first time for a Fronthaul 6020 node in ENM.

— Element Manager Service group restarted as part of ENM upgrade or Rollback.

— User logs out of ENM and relog into ENM.

Solution

1. Select **Add Exception** button.

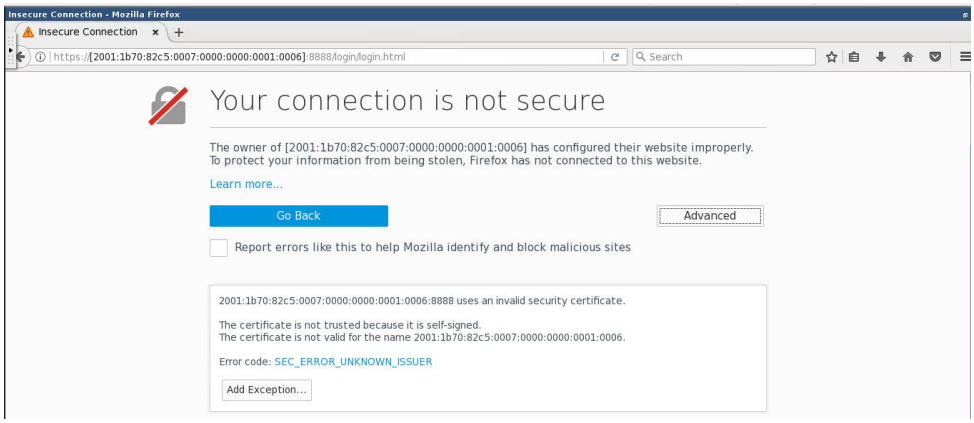


Figure 7 Add Exception

2. Select **Confirm Security Exception**.

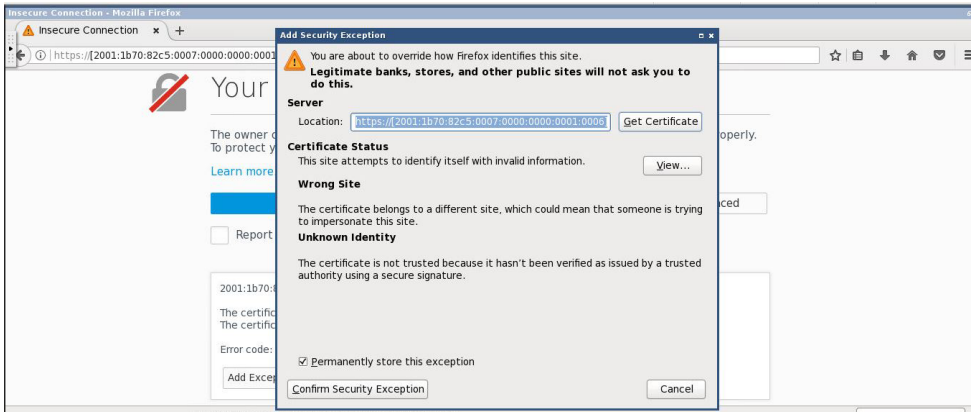


Figure 8 Add Security Exception

3. Login page is displayed in the browser.

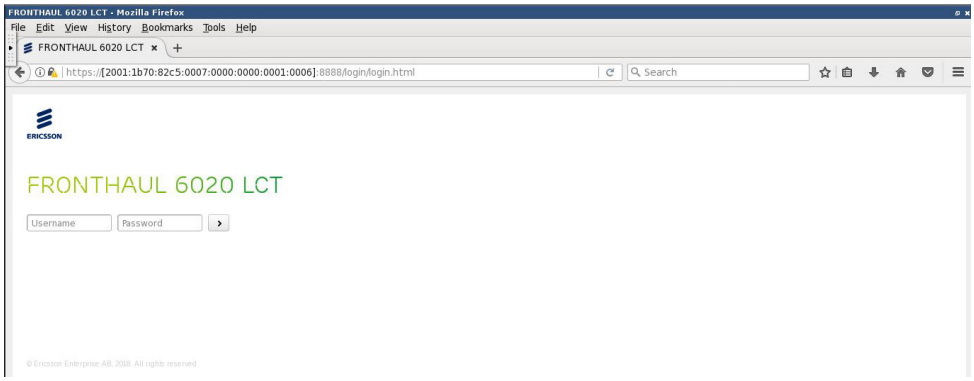


Figure 9 LCT Login

Note: It is optional to log on to LCT by entering user credentials manually.

4. Relaunch the page for auto login into LCT of Fronthaul 6020 node.

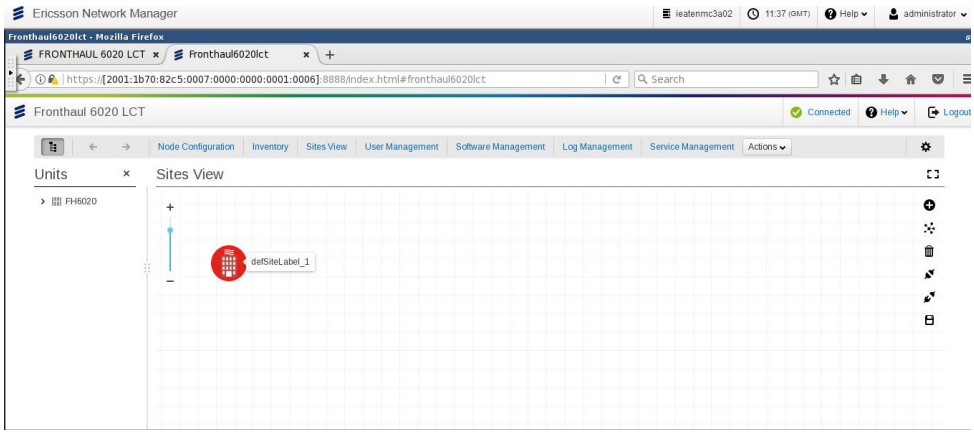


Figure 10 Relaunch Page

7.6 Troubleshooting Flow Automation

This section describes the procedures to diagnose and fix problems encountered when using Flow Automation (FA).

7.6.1 Scripting Building Block Issues

The following sections describe the Scripting Building Block (SBB) issues that a FA user can encounter.

7.6.1.1 Error during SBB Configuration

Cause

The following error occurs when an error is made during SSB configuration.

```
Failed to load the application configuration file.
```

Solution

1. Select the SBB task within the camunda flow `bpmn` file.
2. Go to the **General** tab and look at the **Details** section.
3. Ensure that the following values are correctly configured:

```
Implementation = External
Topic = com.ericsson.oss.services.scripting.fbb.ScriptingBuildingBl →
ock
```

7.6.1.2 Error When Executing SBB Command

Cause

The following error occurs when executing SSB commands.

```
Error while executing the command
```

1. Run the following commands to search logs.

```
[root@scripting-1-internal cloud-user]# cat /ericsson/3pp/jboss/standalone/log/server.l
og | grep -C 5 --color "Error while executing the command :.*., error response:.*."
2019-07-25 12:56:45,324 INFO [com.ericsson.oss.itpf.EVENT_LOGGER] (EJB async - 3) [admi
nistrator, SCRIPTING.BUILDING.BLOCK.RESPONSE.SUCCESS, COARSE, 1253 file input, 3f666b94
-aed3-11e9-a22d-52540058ffe5, [command={
 "discardOutput" : true,
 "timeout" : 300,
 "command" : "/home/shared/administrator/main.sh LTE01dg2ERBS00003"
}, duration=0.00 Minutes]]
```

2. Check input error such as spelling and syntax.
3. Ensure that appropriate token is added to grant access.
4. Consider extending time-out duration.

7.6.1.3 Error When SBB Is Not in Context

Cause

The following error occurs when SBB contextual link is used to view the executed command output within a scripting terminal.

```
SBB contextual link is not working
```

Solution

Change name property value to `faProgressReportVariableNamePrefix`.

7.6.2 Database Issues

The following sections describe the database issues that a FA user may encounter.

7.6.2.1 Database Connection Error

Cause

The following error occurs if the database is not present or unavailable.

```
Error establishing connection to database or schema
```

Solution

1. Open the database connection.

   ```
   [root@flowautomation-1-internal]# PGPASSWORD=fa_pass /opt/rh/postgresql92/root/usr/bin/ →
   psql -h postgresql01 -p 5432 -d flowautomationdb -U fa_admin
   ```

2. View all tables for the active schema (`flowautomationdb`).

   ```
   flowautomationdb=> \d
   ```

3. Check if the `flowautomationdb` is present.

   ```
   flowautomationdb=> select * from fa_db_version
   ```

4. Close the database connection.

   ```
   •flowautomationdb=> \q
   ```

5. Run the initial installation of FA.

   ```
   [root@flowautomation-1-internal]# /ericsson/ERICflowautomationdb_CXP9036276/bin/bash -x →
    flowautomation_db.sh
   ```

7.6.2.2 Database Size Error

Cause

The following error message occurs if there is an error in Database Vacuum and Housekeeping flow.

```
Database size is too large
```

Solution

1. Check the status and process diagram of the Housekeeping flow.
2. Perform data collection on the `flowautomationdb` as described in the ENM Data Collection Guideline.

3. Check status of `flowautomationdb` before and after running vacuum and make sure there is an appropriate difference.
4. Run the following command to check the dB size.

```
[root@<VM>]# PGPASSWORD=fa_pass /opt/rh/postgresql92/root/usr/bin/psql -h postgresql01 -p 5432 -d flowautomationdb -U fa_admin
flowautomationdb=> SELECT pg_size_pretty(pg_database_size('flowautomationdb'));
```

5. Run the Housekeeping flow manually.

7.6.2.3 Recreating Flow Automation Database

Cause

The following errors can occur in a database.

```
Database is oversized.
```

```
Database keeps increasing over time.
```

The possible causes can be the following:

— Database size is too large and it is keeping leftovers from the previous executions.

— Housekeeping internal flow is not succeeding due to a thrown incident.

Do the following troubleshooting analysis.

— — Follow the instructions in the section Connect to a Service on page 2and log on to the Flow Automation VM. If Flow Automation VM is not available, use another VM, for example, scripting VM, which allows you to connect to PostgreSQL.

— Open a Flow Automation dB connection in the VM.

```
PGPASSWORD=fa_pass /opt/rh/postgresql92/root/usr/bin/psql -h postgresql01 -p 5432 -d flowautomationdb -U fa_admin
```

— Check the Flow Automation version.

```
flowautomationdb=> SELECT * FROM fa_db_version;
```

— Check how many flows are registered.

```
flowautomationdb=> SELECT * FROM fa_flow;
```

— Check how many flow executions are present.

```
flowautomationdb=> SELECT * FROM fa_flow_execution;
```

— Check flow automation dB size

```
flowautomationdb=> select pg_size_pretty(pg_database_size('flowautomatio
ndb'));
```

Taking the queries output, check the flows and the executions list. If there is nothing relevant under execution (if flows are old, or all of them are internal), then proceed to clean up.If the database size is greater than 600 MB when FA is not being used, then it is oversized.

— If the Flow Automation ENM application is showing duplicate internal flows, open Flow Automation application, and check how many internal flows are present.

— If Camunda shows incidents within the internal flows, log on to ENM and search if there are incidents reported.

```
https://<ENM>/camunda-flowautomation/app/cockpit/default/#/processes
```

Solution

When FA is not used, truncate the Flow Automation database after the ENM upgrades.

1. Stop JBoss or put Flow Automation VM offline.
   — On a physical environment, connect to LMS and run the following command.

   ```
   /opt/ericsson/enminst/bin/vcs.bsh --offline -g Grp_CS_svc_cluster_flow
   automation
   ```

   Run the following command on LMS to find out on which hostpostgres is online.

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

   — On cloud environment, follow the section, Connect to a Virtual Machine on an ENM on Cloud Deployment on page 3 and log on to the vnflaf.

   Run the following command to find out if postgres is online.

   ```
   consul members | grep -i postgres
   ```

Example

```
vnflaf-services-0 ~]# consul members | grep -i postgres
ieatenmc5b19-postgres-0         10.10.0.117:8301  alive   client  0.9.2  2
       dc1
```

2. Connect to dB.
   - On a physical environment, connect to dB blade from LMS.

     ```
     ssh litp-admin@<db-hostname>
     ```

     Switch to root user.

     ```
     su -
     ```

   - On cloud environment, follow the section, Connect to a Virtual Machine on an ENM on Cloud Deployment on page 3 and log on to the postgres VMand then switch to root user.
3. Run the following command to open a Flow Automation dB connection in the VM.

   ```
   PGPASSWORD=fa_pass /opt/rh/postgresql92/root/usr/bin/psql -h postgresql01 -p 5432 -d fl
   owautomationdb -U fa_admin
   ```

4. Check the Flow Automation version.

   ```
   flowautomationdb=> SELECT * FROM fa_db_version;
   ```

5. Delete Flow Automation dB previous history.

   ```
   flowautomationdb=> DELETE FROM fa_db_version WHERE version>'18.15.1';
   ```

6. Check if the old versions are not present.

   ```
   flowautomationdb=> SELECT * FROM fa_db_version;
   ```

7. Make the Flow Automation dB 18.15.1 version as active.

   ```
   flowautomationdb=> UPDATE fa_db_version SET status=true WHERE version='18.15.1';
   ```

8. Delete the Execution Events table.

   ```
   flowautomationdb=> DROP INDEX "fa_flow_execution_event_target_event_severity";
   flowautomationdb=> DROP INDEX "fa_flow_execution_event_event_severity_target";
   flowautomationdb=> DROP TABLE "fa_flow_execution_event";
   ```

9. JBoss needs to be restarted to re-create the Flow Automation dB. IfFlow Automation VM is offline, make it online again to restartJBoss.

— On a physical environment, connect to LMS as root user and run the following command:

```
/opt/ericsson/enminst/bin/vcs.bsh --online -g Grp_CS_svc_cluster_flowautomation
```

— On cloud environment, follow the section, Connect to a Virtual Machine on an ENM on Cloud Deployment on page 3 and log on to each instance of the flow automation VM and switch to root user.

Run the following command to restart Flow Automation VM.

```
echo "exit 1" > /usr/lib/ocf/resource.d/restart.sh
```

When FA is used, do the following steps on any deployments where the internal flow executions are running with old name pattern or old versions.

10. Follow the instructions in the section Connect to a Service on page 2 and log on to the Flow Automation VM. If Flow Automation VM is not available, use another VM, for example, scripting VM, which allows you to connect to PostgreSQL.

11. Open a Flow Automation dB connection in the VM.

```
PGPASSWORD=fa_pass /opt/rh/postgresql92/root/usr/bin/psql -h postgresql01 -p 5432 -d flowautomationdb -U fa_admin
```

12. Get the latest versions of all internal flows.

```
flowautomationdb=> SELECT flow_id,MAX(version) FROM fa_flow_detail JOIN fa_flow ON fa_flow.id=fa_flow_detail.fa_flow_id WHERE fa_flow.source='INTERNAL' GROUP BY flow_id;
```

Example

```
flow_id | max
-----------------------------------------------------+--------
com.ericsson.oss.fa.internal.flows.stopflowinstance | 1.22.5
com.ericsson.oss.fa.internal.flows.houseKeeping | 1.22.5
com.ericsson.oss.fa.internal.flows.incidentHandling | 1.22.5
```

13. Get the most recent internal flow execution names.

```
flowautomationdb=> SELECT * FROM fa_flow_execution;
```

Example

```
fid | fa_flow_detail_id | process_instance_id | flow_execution_name | executed_by_user
----+-------------------+-------------------------------------+------------ ---------------------------------+-----------------
  1 | 1 | 78b0a864-f723-11e9-99fa-5254009572ce | FA_HOUSE_KEEPING | #Ericsson
  2 | 2 | 79024b10-f723-11e9-99fa-5254009572ce | FA_INCIDENT_HANDLING | #Ericsson
  3 | 4 | 79a2824c-f723-11e9-99fa-5254009572ce | FA_STOP_FLOW_INSTANCE | #Ericsson
54 | 5 | 0d17b2c4-f728-11e9-99fa-5254009572ce | FA_HOUSE_KEEPING2019-10-25 1
```

```
3:05:00.0 | #Ericsson
59 | 7 | 549675fd-f728-11e9-99fa-5254009572ce | FA_STOP_FLOW_INSTANCE2019-10 →
-25 13:07:00.0 | #Ericsson
60 | 6 | 54a28408-f728-11e9-99fa-5254009572ce | FA_INCIDENT_HANDLING2019-10- →
25 13:07:00.0 | #Ericsson
(6 rows)
```

14. Update the most recent internal flow execution names with pattern _version (underscore version).

    Example

```
flowautomationdb=> UPDATE fa_flow_execution SET flow_execution_name='FA_INCI →
DENT_HANDLING_1.22.5' WHERE id=60;
or
flowautomationdb=> UPDATE fa_flow_execution SET flow_execution_name='FA_HOUS →
E_KEEPING_1.22.5' WHERE id=54;
or
flowautomationdb=> UPDATE fa_flow_execution SET flow_execution_name='FA_STOP →
_FLOW_INSTANCE_1.22.5' WHERE id=59;
```

Note:
- Use the newer version time stamp to pick and choose the right ID.
- The changes are done to address manually the dB inconsistencies.

7.7 Troubleshooting Configuration Management Treat-As

This section describe the steps to diagnose and fix common problems of Configuration Management (CM) Treat-As use cases.

7.7.1 OSS Model Identity Updates When Models Are Same across Different Releases of the Nodes

Network Element can be added in ENM with or without specifying OSS Model Identity (OMI).

When OMI is specified, node is synchronized against the related version in ENM. If OMI is not specified, an appropriate release is identified during synchronization based on the product data on the node.

When node models are same across different releases of the nodes, expected OMI updates after CM synchronization are described in the ENM Operator's Guide.

Forward Compatibility alarm is raised after CM synchronization if there is a difference in the updated node product version and the product version referred from the OMI.

Note: Check the node product version in the Network Element `neProductVersion` attribute for managed software release information of the node.

Fronthaul 6020 is the node that supports this behavior in ENM.

7.7.1.1 ENM Is Managing Nodes with Supported Software Release

OMI Is Not Set When Adding Node for the First Time in ENM

After CM synchronization, Network Element OMI is updated to the released version on the node.

For example, if a node is running with 18.Q4 release version, node is synchronized into ENM with 18.Q4 and OMI is set to 18.Q4. If a node is running with 18.Q3 release version, node is synchronized into ENM with 18.Q3 and so on.

OMI Is Set When Adding Network Element in ENM

After CM synchronization, Network Element OMI is not modified although node has a different release version.

For example, if the node is running with 18.Q4 release version and OMI is set to 18.Q3, after CM synchronization, node is synchronized into ENM with 18.Q4 but OMI remains as 18.Q3.

In general, if an OMI is set in ENM, even if the node release changes (node software upgrade/downgrade) but the model has not changed compared to the model associated to the currently set OMI, OMI is not updated after CM synchronization.

Node Is Discovered Using Node Discovery Application in ENM

When a node is discovered through Node Discovery application with CM enabled, all the nearest OMIs are resolved and least of the resolved model identities is set by default.

After CM synchronization, Network Element OMI is not modified even though node has different release version.

For example, if the node is running with 18.Q4 release version and OMI is set to least supported OMI 18.Q2 as part of node discovery, after CM synchronization, node is synchronized into ENM with 18.Q4 but OMI remains as 18.Q2.

7.7.1.2 ENM Is Managing Nodes Which has Unsupported Software Release

OMI is Not Set When Adding Node for the First Time in ENM

After CM synchronization, Network Element OMI is updated to the latest supported software release in ENM.

For example, if a node is running with 19.Q2 unsupported release version, node is synchronized into ENM with 18.Q4 and OMI is set to 18.Q4.

OMI Is Set When Adding Network Element in ENM

After CM synchronization, Network Element OMI is not modified although node has a different release version.

For example, if the node is running with 18.Q4 release version and OMI is set to 18.Q3, after CM synchronization, node is synchronized into ENM with 18.Q4 but OMI remains as 18.Q3.

Node Is Discovered Using Node Discovery Application in ENM

When a node is discovered through Node Discovery application with CM enabled, all the nearest OMIs are resolved and least of the resolved model identities is set by default.

After CM synchronization, Network Element OMI is not modified even though node has different release version.

For example, if the node is running with 18.Q4 release version and OMI is set to least supported OMI 18.Q2 as part of node discovery, after CM synchronization, node is synchronized into ENM with 18.Q4 but OMI remains as 18.Q2.

7.8 Troubleshooting Help Search

This section describes the troubleshooting scenarios related to the recovery of Help Search.

7.8.1 Recover Indexing for ENM Help Center Search

Prerequisites

Root access to dB clusters.

Cause: Diagnostics

— Check the status of elasticsearch service.

```
[root@cloud-db-1 ~]# hagrp -state Grp_CS_db_cluster_elasticsearch_clustered_service

#Group Attribute System Value
Grp_CS_db_cluster_elasticsearch_clustered_service State cloud-db-1 |ONLINE|
```

If indexes are present, run the following command.

```
[root@cloud-db-1 ~]# curl -s elasticsearch:9200/_cat/indices?v
```

```
health status index uuid pri rep docs.count docs.deleted store.size pri.store.size
green open enm-help-search oJchrZsGTqyqXSEJLqrkoQ 1 0 1964 0 5.1mb 5.1mb
green open enm_logs-application-2019.10.22 MjvH9x5PQm-PxGJJw8kp1A 1 0 13195 0 2.9mb 2.9 →
mb
green open enm_logs-application-2019.12.17 SmAZa06FTs-ovxcHD8FZvw 1 0 689324 0 194.3mb →
194.3mb
green open enm_logs-application-2019.12.18 plzL_KbLS3CiAqzP5UQC5g 1 0 1013732 0 248mb 2 →
48mb
```

If the `enm-help-search` line is not in the list, the indexes are not present.

Solution

1. Remove `enm-help-search` indexes.

```
[litp-admin@cloud-db-1 ~]$ curl -X DELETE "elasticsearch:9200/enm-help-search?pretty"
{
  "acknowledged" : true
}
```

2. Check and remove the file lock. On VM where help-search is running (`httpd` on physical or `guicore` on cloud), run the following commands.

```
[cloud-user@svc-7-httpd bin]$ sudo ls -la /ericsson/enm/dumps/.ea.lck
```

The following output is displayed if the lock is not present.

```
# ls: cannot access /ericsson/enm/dumps/.ea.lck: No such file or directory
```

If the lock is present, remove it using the following command.

```
# sudo rm /ericsson/enm/dumps/.ea.lck
```

3. Start indexing using the following commands.

```
[cloud-user@svc-7-httpd bin]$ cd /ericsson/eagleanalyzer/bin
[cloud-user@svc-7-httpd bin]$ sudo ./eagle_launcher.sh start
```

Example

```
cloud-user[2722]: Executing ./eagle_launcher.sh start
cloud-user[2727]: /ericsson/tor/data/global.properties exists!
cloud-user[2745]: Starting Eagle Analyzer:
cloud-user[2746]: /usr/java/latest/bin/java -server -Xmx1024M -Dfile.encoding=UTF-8 -Do →
rg.slf4j.simpleLogger.defaultLogLevel=none
-Djava.ext.dirs=/ericsson/eagleanalyzer/lib:/ericsson/3pp/commons-codec/lib:/ericsson/3 →
pp/httpclient/lib:/ericsson/3pp/httpcore/lib:/ericsson/3pp/jackson/lib:/ericsson/3pp/js →
oup/lib com.ericsson.oss.itpf.eagle.core.Core
--config /ericsson/eagleanalyzer/conf/help-sdk-enm-es.json
cloud-user[2761]: Eagle Analyzer is running with pid 2747
```

Refresh the ENM page before trying the **`Help Search`** again.

7.9 Troubleshooting SNMP Connectivity Issues for SNMP-based Network Elements

This section describes the troubleshooting scenarios-related Network Elements, which are configured with SNMPv1/SNMPv2c/SNMPv3 protocol for connectivity toward nodes to execute SNMP-based use cases.

7.9.1 SNMP Connection Failures during Connectivity or Discovery Phase

Depending on Network configuration, SNMP-based FCAPS use cases like CM Synchronization, SHM backup/ restore/ software upgrade/ import license, FM configuring target destination, FM alarms synchronizing, PMIC activation/ deactivation/ file collection could fail reporting SNMP connectivity issues in the logs.

The following section outlines the configurable parameters, which can help to tune the connection timeout to solve issues that may arise during SNMP connectivity phase as part of any SNMP based use case execution.

7.9.1.1 Update SNMPv1/SNMPv2c/SNMPv3 Target Timeout and Retry Parameters

> Mediation applications uses the configured values described in the following table for new SNMPv1/SNMPv2c/SNMPv3 connection creation towards node as part of SNMP based FCAPS use case execution.

Table 2 Parameter Description

Parameter Name	Default Value	Description	Node Types Support
minilinkIndoorSnmpFmRetries	1	Number of SNMP target retry count.	MINI-LINK TN, MINI-LINK LH, MINI-LINK CN210, MINI-LINK CN510R1, MINI-LINK CN810R1, MINI-LINK CN810R2, MINI-LINK CN510R2, MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693,MINI-LINK 6291, MINI-LINK 6694, MINI-LINK 6651 , MINI-LINK 6654, MINI-LINK 6655, MINI-LINK 6366
minilinkIndoorSnmpFmTimeout	15	Number of SNMP target wait interval in seconds.	
fronthaulSnmpFmRetries	1	Number of SNMP target retry count.	Fronthaul 6080, Fronthaul 6020
fronthaulSnmpFmTimeout	15	Number of SNMP target wait interval in seconds.	
snmpCmConnectionRetries	1	Number of SNMP target retry count.	MINI-LINK 6351, MINI-LINK 6352, MINI-LINK PT2020, Switch 6391, MINI-LINK TN, MINI-LINK LH, MINI-LINK CN210,MINI-LINK CN510R1,MINI-LINK CN810R1,MINI-LINK CN810R2,MINI-LINK
pm_snmpConnRetries	1	Number of SNMP target retry count.	
pm_snmpTimeOut	15	Number of SNMP target wait interval in seconds.	

Parameter Name	Default Value	Description	Node Types Support
			CN510R2, MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693,MINI-LINK 6291, MINI-LINK 6694, MINI-LINK 6651 , MINI-LINK 6654, MINI-LINK 6655, MINI-LINK 6366, JUNIPER-MX,JUNIPER-SRX,JUNIPER-PTX,JUNIPER-vMX,JUNIPER-vSRX, CISCO-ASR9000 Series, CISCO-ASR900 Series

Table 3 CmNodeHeartbeatSupervision Attribute Description

CmNodeHeartbeatSupervision Attribute(s)(1)	Default Value	Description
heartbeatTimeout	15	Duration after which heartbeat check will be timed out in seconds..

(1) For tuning the SNMP connection, timeout for SNMP based nodes managed in mssnmpcm, CmNodeHeartbeatSupervision managed object attribute(s) to be updated using model driven tools (CM CLI, Topology Browser or Network Explorer).

7.9.1.2 Update SNMPv3 Session Timeout and Retry Parameters

> SNMPv3 connection requires additional discovery phase. Mediation applications uses the configured values described in the following table for every new SNMPv3 connection creation towards node as part of SNMP based FCAPS use case execution.

Table 4 Parameter Description

Parameter Name	Default Value	Description (1)	Node Types Support
snmpCmSessionRetries	1	Value of SNMPv3 session retries used during establishing SNMPv3 connection.	MINI-LINK 6351, MINI-LINK 6352, MINI-LINK PT2020, Switch 6391, MINI-LINK TN, MINI-LINK LH, MINI-LINK CN210,MINI-LINK CN510R1,MINI-LINK CN810R1,MINI-LINK CN810R2,MINI-LINK CN510R2, MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693,MINI-LINK 6291, MINI-LINK 6694, MINI-LINK 6651 , MINI-LINK 6654, MINI-LINK 6655, MINI-LINK 6366, JUNIPER-MX, JUNIPER-SRX, JUNIPER-PTX, JUNIPER-vMX, JUNIPER-vSRX, CISCO-ASR9000 Series, CISCO-ASR900 Series
snmpCmSessionTimeout	15000	Value of SNMPv3 session timeout in milliseconds used during establishing SNMPv3 connection.	

Parameter Name	Default Value	Description (1)	Node Types Support
pm_snmpSessionRetries	1	Value of SNMPv3 session retries used during establishing SNMPv3 connection.	MINI-LINK TN, MINI-LINK LH, MINI-LINK CN210,MINI-LINK CN510R1,MINI-LINK CN810R1,MINI-LINK CN810R2,MINI-LINK CN510R2, MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693,MINI-LINK 6291, MINI-LINK 6694, MINI-LINK 6651 , MINI-LINK 6654, MINI-LINK 6655, MINI-LINK 6366, JUNIPER-MX, JUNIPER-SRX, JUNIPER-PTX, JUNIPER-vMX, JUNIPER-vSRX, CISCO-ASR9000 Series, CISCO-ASR900 Series
pm_snmpSessionTimeout	15000	Value of SNMPv3 session timeout in milliseconds used during establishing SNMPv3 connection.	
minilinkIndoorSnmpFmSessionRetries	1	Value of SNMPv3 target retries used during establishing SNMPv3 connection.	MINI-LINK TN, MINI-LINK LH, MINI-LINK CN210,MINI-LINK CN510R1,MINI-LINK CN810R1,MINI-LINK CN810R2,MINI-LINK CN510R2, MINI-LINK 6691, MINI-LINK 6692, MINI-LINK 6693,MINI-LINK 6291, MINI-LINK 6694, MINI-LINK 6651 , MINI-LINK 6654, MINI-LINK 6655, MINI-LINK 6366
minilinkIndoorSnmpFmSessionTimeout	15000	Value of SNMPv3 session timeout in milliseconds used during establishing SNMPv3 connection.	

(1) SNMP 3PP used in ENM follows "exponential back off" algorithm to calculate the SNMPv3 connection timeout given the initial value and the number of retries as mentioned.

In general, if the timeout value is 'T' and the retry value is 'R', the total time taken for the entire SNMP operation can be given as

$$\text{Total time taken} = \sum_{r=0}^{r=R} T \times 2^{r}$$

It is recommended to keep the total time taken within 2 minutes to avoid mediation application being blocked due to connectivity timeout issues.

7.10 NCM Logging Information

NCM produces log reports suitable for analysis by end users and system administrators when issues are encountered.

Each NCM server maintains its own set of the following logs.

— JBoss server logs are stored in the `/opt/ericsson/ncm/jboss-7.4.0.Final/standalone/log` directory. The `server.log` file includes information about when the server starts and whether the node inventory synchronization task is complete or not. The file is overwritten each time JBoss restarts. Up to six generations of this file are maintained. A new generation starts when the main `server.log` file exceeds 50 MB. The total amount of space allowed for the log files is 300 MB.

Every access to the application server is logged with the following details:

- Time stamp at which the request took place.
- Source IP Address from where the request was raised.
- User account (if known) of who made the request.
- URL requested.
- HTTP response code for the request sent.

The log can be found at the location `/opt/ericsson/ncm/jboss-7.4.0.Final/standalone/log/default-host` and the default name of the log is `access_log.<YYYY-MM-DD>`.

- NCM DMI server logs are stored in the `/opt/ericsson/ncm/app/log/dmi` directory. DMI server logs are kept for the current session and the previous session only. Each time the NCM DMI server starts, the NCM DMI server logs from the previous session are moved from this directory to the `dmi/OLD` subdirectory and overwrite the current contents.
- Log files generated by the `app-admin.ksh` script are stored in `/opt/ericsson/ncm/app/log/dmi`. The NCM client log is maintained on the client computer in the home directory of each user.

7.10.1 Accessing NCM Logging Information

Prerequisites

- Authority to work as a system administrator having root access to the platforms.
- Ensure that you are logged on the Network Connectivity Manager server as NCM user to run the `app-admin.ksh` script. If not, log on using the following command.

```
su ncmuser
```

Solution

1. Connect to ncm Service Group. Refer to ENM System Administrator Guide to find how to connect to a Service Group.
2. Log files are divided in current logs and historical logs, and their snapshots collected every three hours and organized in a dedicated folder in a shared file system. The NCM application keeps the latest seven days of logs and automatically rotate them removing the old ones.
   - The current logs are stored in the `/opt/ericsson/ncm/app/log` directory.

- Historical logs are stored under the `/ericsson/ncm/log/history` directory.
  - Logs of previous days are stored in `tar.gz` files named as `Logs.YYYY-MM-DD-HH-MM-SS.tgz`.
  - Logs for the current day are copied every three hours in the folder named `latest`, grouped in directories created every three hours and named `HOUR_03`, `HOUR_06`. Every such directory contains a snapshot copy of the application log files as they are presented in the `/opt/ericsson/ncm/app/log` directory at that time of the day.
  - The EM directory contains a set of sub-directories, one per NE, with the relevant log files related to the latest successful synchronization of NE information. Therefore, from these log files it is possible to verify the information that is currently managed by the NCM application for that NE.

3. The `ericsson/enm/dumps/ncm` directory may contain jboss crash dumps if jboss crashes.
4. All output information from the startup when a server boots or reboots can be found as entries inside the `/var/log/boot.msg` file.

7.11 Troubleshooting Transport Topology Name Conflict Error

Use this procedure to troubleshoot when Transport Topology is not visible in the Custom Topology tree in the Topology Browser.

This can be caused by a name conflict with "TransportTopology". Confirm the issue by observing the following error message in LogViewer:

```
"A collection with the name <Default Value> already exists. Transport topology c →
ould not be created. Please follow the troubleshooting guide to resolve this iss →
ue."
```

If a topology has already been created with the name TransportTopology the user will see the above error.

Diagnosis:

1. Enter Log Viewer
2. Use the search tab to search for the error.
   a. 'A collection with the name <Default Value> already exists. Transport topology could not be created. Please follow the troubleshooting guide to resolve this issue.'.
   b. Filter the results by Error and Info to display only the Error and Info Messages.

3. Verify there is a name conflict error.

To resolve this issue, the user must change the default value of the `customTopologyName` parameter in the PIB to the name you wish to give to CustomTopology. No other Collection should exist with this name, whether private or public.

For instruction on how to change the default value of `customTopologyName` refer to *Change Default customTopologyName Value* in ENM System Administrators Guide[1].

7.12 Troubleshooting HTTP Status 404 Error When Launching ENM

Use this procedure to clear the `HTTP Status 404` error that may occur if some of the ENM services are registered as root context to `mod_cluster`.

Prerequisites

— Access to the Management Server (MS) and Peer Nodes.

— Basic knowledge of Linux and Networking.

Steps

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

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

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

   In cloud :
   # ssh cloud-user@<VNF-LAF server IP>
   ```

2. Execute below command for all available `httpd` instances to identify which VM has registered its context with `httpd modcluster` as root:

   ```
   curl -X GET http://httpd-instance-*:8666/mod_cluster-manager >> <file path o →
   utput to be stored>.html
   ```

   For Example:

   ```
   curl -X GET http://httpd-instance-1:8666/mod_cluster-manager >> <file path o →
   utput to be stored>.html
   ```

Note: On the event of failure, change the domain name from `httpd-instance` to `httpd-internal` depending on the active SVC.

3. Identify the VM which context is registered with root `"/ "`.

   Sample Output:

```
Balancer: uicluster,LBGroup: ,Flushpackets: Off,Flushwait: 10000,Ping: 10000 →
000,Smax: 61,Ttl: 60000000,Status: OK,Elected: 0,Read: 0,Transferred: 0,Conn →
ected: 0,Load: 1
Virtual Host 1:
Contexts:
 /, Status: ENABLED Request: 0
 Aliases:
 default-host
Node cb4302e5-6028-3ca8-ae28-3b88c5b01841 (ajp://10.10.0.182:8009):
```

4. Connect to the VM using Connect to a Service on page 2 section and execute below command to restart service.

```
# service jboss restart
```

5. Relaunch Ericsson Network Manager.

7.13 Troubleshooting HA Proxy IPv6 NBI

> This topic describes how to troubleshoot issues associated with IPv6 connectivity on the Northbound Interface of ENM web services.

Prerequisites

— User requires access to the Management Server (MS) and Peer Nodes.

— User requires basic knowledge of Linux and Networking.

Result

User is able to troubleshoot issues related to IPv6 connectivity to the NBI web services.

Troubleshooting Tasks

The sections below provide information about the troubleshooting tasks required for the following issues:

7.13.1 Gather Information about the Deployment

1. Log on to MS as the `litp-admin` user and query the deployment model to retrieve the IPv6 address assigned as the VIP for the `haproxy-ext` service.

```
[litp-admin@ms-1 ]$ litp show -p /deployments/enm/clusters/svc_cluster/servi →
ces/haproxy-ext/ipaddresses/haproxy-ext_vipv6 -o ipaddress
2001:1b70:82a1:146:0:609:5326:50
```

2. Log on to one of the Peer Nodes in the svc cluster (for example. `svc-1`) and switch to the root user.

```
[litp-admin@ms-1 ]$ ssh litp-admin@svc-1
[litp-admin@ieatrcxb5032 ~]$ su root
```

3. Execute the following commands to check that the `haproxy-ext` service is online and to identify the peer node it is running on:

```
[root@ieatrcxb5032 ]# hastatus -sum | grep haproxy_ext
B  Grp_CS_svc_cluster_haproxy_ext ieatrcxb5032         Y          N           →
      ONLINE
B  Grp_CS_svc_cluster_haproxy_ext ieatrcxb5033         Y          N           →
      OFFLINE
```

   If `haproxy-ext` is online on a different node, log on to that node and switch to root user before continuing to the next task.

7.13.2 Check the Server Side Network Configuration Settings and Network Health

1. Check that the VIP is one of the IPv6 addresses on the system and that the device it is assigned to is running.

```
[root@ieatrcxb5032 ]# ip -o -6 address show | egrep 'scope (site|global)'
7: br0    inet6 2001:1b70:82a1:146:0:609:5326:f/64 scope global \       vali →
d_lft forever preferred_lft forever
7: br0    inet6 2001:1b70:82a1:146:0:609:5326:50/64 scope global \       val →
id_lft forever preferred_lft forever
7: br0    inet6 2001:1b70:82a1:146:0:609:5326:1/64 scope global \       vali →
d_lft forever preferred_lft forever

[root@ieatrcxb5032  ]# ip link show br0
7: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNO →
WN
    link/ether 8c:dc:d4:1d:68:c0 brd ff:ff:ff:ff:ff:ff
```

2. For connection issues from remote systems, check that a valid default gateway is contactable and on the same subnet.

```
default via 2001:1b70:82a1:146:0:609:0:1 dev br0  metric 1024  mtu 1500 advm →
ss 1440 hoplimit 4294967295

[root@ieatrcxb5032 ]# ping6 -c 3 2001:1b70:82a1:146:0:609:0:1
PING 2001:1b70:82a1:146:0:609:0:1(2001:1b70:82a1:146:0:609:0:1) 56 data byte →
s
64 bytes from 2001:1b70:82a1:146:0:609:0:1: icmp_seq=1 ttl=64 time=11.0 ms
64 bytes from 2001:1b70:82a1:146:0:609:0:1: icmp_seq=2 ttl=64 time=0.323 ms
```

```
64 bytes from 2001:1b70:82a1:146:0:609:0:1: icmp_seq=3 ttl=64 time=0.338 ms

--- 2001:1b70:82a1:146:0:609:0:1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.323/3.917/11.090/5.072 ms[root@ieatrcxb5032 ]# ip -
6 route | grep default
```

3. Find the process ID of the `haproxy-ext` service and check that it is bound to listen on the VIP address.

```
[root@ieatrcxb5032  ]# ps aux | grep haproxy-ex[t]
haproxy  26511  1.7  0.0  55044 10308 ?        Ss   Aug07  38:58 /usr/sbin/h
aproxy -D -f /ericsson/3pp/haproxy/data/config/haproxy-ext.cfg -p /var/run/h
aproxy-ext.pid

[root@ieatrcxb5032  ]# netstat -A inet6 -ntlp | grep 26511
tcp        0      0 2001:1b70:82a1:146:0:609:5326:50:80 :::*
    LISTEN      26511/haproxy
tcp        0      0 2001:1b70:82a1:146:0:609:5326:50:443 :::*
    LISTEN      26511/haproxy

[root@ieatrcxb5032  ]# lsof -p 26511 -a -i 6
COMMAND   PID    USER   FD   TYPE  DEVICE SIZE/OFF NODE NAME
haproxy 26511 haproxy    5u  IPv6 2347356      0t0  TCP [2001:1b70:82a1:146:
0:609:5326:50]:http (LISTEN)
haproxy 26511 haproxy    7u  IPv6 2347358      0t0  TCP [2001:1b70:82a1:146:
0:609:5326:50]:https (LISTEN)
```

4. Ensure that the firewall allows incoming traffic on the http (80) and https (443) ports.

```
[root@ieatrcxb5032  ]# ip6tables -nL INPUT| egrep -w 'dports.*(443|80)'
ACCEPT     tcp      ::/0                ::/0                multiport dport
s 443 /* 019 ssltcp ipv6 */ state NEW
ACCEPT     tcp      ::/0                ::/0                multiport dport
s 80 /* 996 httpd v6 */ state NEW
```

7.13.3 Check the Client Side Network Configuration Settings and Network Health

1. Ensure that the VIP address of the `haproxy-ext` service is the IPv6 address that the FQDN is resolves to.

```
[root@xyz1111  ]# host enmapache.athtem.eei.ericsson.se
enmapache.athtem.eei.ericsson.se has address 131.160.146.183
enmapache.athtem.eei.ericsson.se has IPv6 address 2001:1b70:82a1:146:0:609:5
326:50
```

2. Check that the client has an IPv6 address and a valid default gateway for IPv6 traffic.

```
[root@xyz1111  ]# ip -o -6 address show | egrep 'scope (site|global)'
2: eth1    inet6 2001:1b70:82a1:103::1/64 scope global \       valid_lft for
ever preferred_lft forever

[root@xyz1111  ]# ip -6 route | grep default
default via 2001:1b70:82a1:103:0:609:0:1 dev br0  metric 1024  mtu 1500 advm
ss 1440 hoplimit 4294967295

[root@xyz1111  ]# ping6 -c 1 2001:1b70:82a1:103:0:609:0:1
PING 2001:1b70:82a1:146:0:609:0:1(2001:1b70:82a1:103:0:609:0:1) 56 data byte
s
64 bytes from 2001:1b70:82a1:103:0:609:0:1: icmp_seq=1 ttl=64 time=11.0 ms
```

7.13.4 Test Connectivity Between the Client and the Server

1. Check that there are no local firewall rules that block outbound connections toward the remote VIP address.

```
[root@xyz1111  ]# ip6tables -nL
...
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
<list_of_rules_to_inspect>
```

2. Check that the VIP address is accessible and responding.

```
[root@xyz1111  ]# ping6 -c 3 2001:1b70:82a1:146:0:609:5326:50
PING 2001:1b70:82a1:146:0:609:5326:50 (2001:1b70:82a1:146:0:609:5326:50) 56 →
data bytes
64 bytes from 2001:1b70:82a1:146:0:609:5326:50: icmp_seq=1 ttl=64 time=11.0 →
ms
64 bytes from 2001:1b70:82a1:146:0:609:5326:50: icmp_seq=2 ttl=64 time=0.323 →
 ms
64 bytes from 2001:1b70:82a1:146:0:609:5326:50: icmp_seq=3 ttl=64 time=0.338 →
 ms

--- 2001:1b70:82a1:146:0:609:0:1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.323/3.917/11.090/5.072 ms
```

3. Check that it is possible to connect to HTTP port (80) on the remote VIP address.

```
[root@xyz1111  ]# curl -v6k http://enmapache.athtem.eei.ericsson.se

About to connect() to enmapache.athtem.eei.ericsson.se port 80 (#0)

* Trying 2001:1b70:82a1:146:0:609:5326:50... connected

* Connected to enmapache.athtem.eei.ericsson.se (2001:1b70:82a1:103::80) por →
t 80 (#0)

> GET / HTTP/1.1

> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.14. →
0.0 zlib/1.2.3 libidn/1.18 libssh2/1.4.2

> Host: enmapache.athtem.eei.ericsson.se

[...]

<html><head>

<title>302 Found</title>

</head><body>

<h1>Found</h1>

<p>The document has moved <a href="https://enmapache.athtem.eei.ericsson.se: →
443/login/?goto=http%3A%2F%2Fenmapache.athtem.eei.ericsson.se%3A80%2F">here< →
/a>.</p>

</body></html>

Connection #0 to host enmapache.athtem.eei.ericsson.se left intact

Closing connection #0
```

4. Check that it is possible to connect to the HTTPS port (80) on the remote VIP address.

```
[root@xyz1111  ]# curl -v6k https://enmapache.athtem.eei.ericsson.se/login/? →
goto=https://enmapache.athtem.eei.ericsson.se

* About to connect() to enmapache.athtem.eei.ericsson.se port 443 (#0)

* Trying 2001:1b70:82a1:146:0:609:5326:50... connected

* Connected to enmapache.athtem.eei.ericsson.se (2001:1b70:82a1:103::80) por →
t 443 (#0)

[...]

> GET /login/?goto=https://enmapache.athtem.eei.ericsson.se HTTP/1.1

> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.14. →
0.0 zlib/1.2.3 libidn/1.18 libssh2/1.4.2

> Host: enmapache.athtem.eei.ericsson.se

> Accept: */*

[...]

<html>

<head>

<title>ENM Login</title>

[...]

</body>

* Connection #0 to host enmapache.athtem.eei.ericsson.se left intact

* Closing connection #0
```

Note: When executing the `ping6` or `curl` commands, it may be useful to monitor traffic on the service side to confirm that ICMP or TCP packets are arriving.

The following are example commands for monitoring ICMP6 and HTTP/HTTPS traffic over IPv6 (root privileges are required):

- `tcpdump -ni any icmp6`
- `tcpdump -ni br0 icmp6 and host 2001:1b70:82a1:146:0:609:5326:50`

Reference List

[1] *ENM System Administrator Guide*, 1/1543-AOM 901 151

[2] *ENM Network Integration Guideline*, 1/102 72-AOM 901 151.

[3] *ENM Operator's Guide*, 1/1553-AOM 901 151

[4] *ENM Security System Administrator Guide*, 2/1543-AOM 901 151

[5] *VNF-LCM Installation Instructions*, 1/1531-CNA 403 3313, available in the ENM Installation and Support CPI Library.

[6] *Typographic Conventions*, 3/1551-FCK 101 05

[7] *ENM Backup and Restore System Administrator Guide*, 3/1543-AOM 901 151

[8] *ENM Configuration System Administrator Guide*, 1/1543-AOM 901 151-1

[9] *ENM Data Collection Guideline*, available from local Ericsson Support.

[10] *ENM Interwork Description for File Lookup Service (FLS)*, 1/155 19-CNA4033301

[11] *ENM Performance Management System Administrator Guide*, 1/1543-AOM 901 151-3

[12] *ENM Installation Instructions*, Available from local Ericsson Support

[13] *Manage Security User Guide*, *18/1553-LZA 701 6014*, available from relevant WCDMA RAN CPI Library.

[14] *ENM Configuration Troubleshooting Guide*, 1/159 01-AOM 901 151-1

[15] *ENM Monitoring Troubleshooting Guide*, 1/159 01-AOM 901 151-2

[16] *ENM Performance Management Troubleshooting Guide*, 1/159 01-AOM 901 151-3

[17] *ENM Security Management Troubleshooting Guide*, 1/159 01-AOM 901 151-4

[18] *ENM on Cloud Backup and Restore Administrator Guide*, 5/1543-AOM 901 151

[19] *ENM Troubleshooting Guide*, 1/159 01-AOM 901 151

[20] *ENM Identity and Access Management System Administrator Guide*, 2/1543-AOM 901 151-1

[21] *ENM Network Security Configuration System Administrator Guide*, 2/1543-AOM 901 151-2

[22] *ENM Public Key Infrastructure System Administrator Guide*, 2/1543-AOM 901 151-3

[23] *OSS-RC Configuration for ENIQ*, 1/1546-AOM 901 076, available from Ericsson Network IQ Events CPI Library.

[24] *ENM Identity and Access Management Programmers Guide*, 19817-cna 403 3016

[25] *ENM Product Description*, 1/1551-AOM 901 151

[26] *ENM Monitoring System Administrator Guide*, 1/1543-AOM 901 151-2

[27] *LITP Node Hardening Instructions*, 2/1531-CSA 113 110

[28] *CAS Software Dropbox End-User Guide*, 6/1553-HSC 901 110, available from Ericsson Support.
[29] *ENM Neo4j Troubleshooting Guide*159 01-CNA 403 3405
[30] *ENM System Monitor User Guide*, 1/1553-cna 403 3115
[31] ENM NIG Connection Matrix
[32] *ENM System Security Configuration Programmers Guide*
1/19817-cna 403 3065 Uen
[33] *Neo4j Documentation*
https://support.neo4j.com/hc/en-us/articles/360006361794-Causal-Cluster-FAQ-for-heavy-workloads
[34] *ENM Parameter List*, 1/19059-AOM 901 151
[35] *Managed Object Model (MOM) RNC*, 155 54-CXC 173 5901/1-V1
[36] *SAPC, Measurements Ericsson Service-Aware Policy Controller User Guide*, 1/15553 - AXB 901 33/7
[37] *SAPC, Managed Object Model*, 155 54-LZN 708 0672/5-V1
[38] *ENM Privacy User Guide*, 2/1553-AOM 901 151