ERICSSON

ENM Security Management Troubleshooting Guide

Check List

1/159 01-AOM 901 151-4 Uen AK

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 ENM Security Management Troubleshooting Guide

This document describes the system troubleshooting tasks for ENM Security Management.

Target Group

System Administrator

2 Credential Manager Troubleshooting

This section provides the troubleshooting steps recommended to diagnose and fix common problems in Credential Manager CLI.

2.1 `credm` Command Returns `404 Not Found` Error

This task resolves the `404 Not Found` issue after the execution of a generic `credm` command.

Prerequisites

— A command window has been opened and the user has super user privileges.

  See the *Connect to a Virtual Machine* section in ENM Troubleshooting Guide, Reference [19] for further information on how to connect to the required VM.

Steps

On physical environment:

1. Check the status of the `CMServ` service on an SVC node.

   In this example the node is the `SVC-1`:

   ```
   [root@cloud-svc-1 ~]# hagrp -state | grep cmserv
   ```

2. Switch the status to `ONLINE` if the `CMServ` service status is `OFFLINE`.

   ```
   [root@cloud-svc-1 ~]# hagrp -online Grp_CS_svc_cluster_cmserv -sys cloud-svc →
   -1
   ```

3. Check the status of the `CMServ` service on the SVC node.

   ```
   [root@cloud-svc-1 ~]# hagrp -state | grep cmserv
   ```

4. Retry the `credm` command if the `CMServ` service status is `ONLINE`.

On cloud environment:

5. Copy the key to the `emp` server using the private key for authentication. Log on `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 ~]$ sudo su -
[root-user@ostk003-emp-0 ~]# consul members | grep cmserv
cmserv-0             10.5.1.62:8301   alive   client  0.8.1  2         dc1
cmserv-1             10.5.1.63:8301   alive   client  0.8.1  2         dc1
```

Verify that at least one instance of `cmserv` service is in `alive` state.

If all instances are `failed` or `left`, wait for HA recovery. SAM finds the failure and triggers a HA workflow.

The service instance state moves from `failed` to `left` and then to `alive`.

Results

The `404 Not Found` error is not raised after the execution of `credm` command.

2.2 `credm` Command Returns an Internal Error

> This task resolves a generic internal error issue after the execution of a generic `credm` command.

Prerequisites

— A command window has been opened and the user has super user privileges.

See the *Connect to a Virtual Machine* section in ENM Troubleshooting Guide, Reference [19] for further information on how to connect to the VM.

Steps

On physical deployment:

1. Check the status of each SPS service.

   In this example the nodes are the `SVC-1` and the `SVC-2`:

   ```
   [root@cloud-svc-1 ~]# hagrp -state | grep sps
   ```

   The system returns the status of all the SPS services.

2. Switch it to `ONLINE` on any SVC node if the status of all the SPS services is `OFFLINE`, otherwise go to step 3.

   ```
   [root@cloud-svc-1 ~]# hagrp -online Grp_CS_svc_cluster_sps -sys cloud-svc-1
   ```

   ```
   [root@cloud-svc-1 ~]# hagrp -online Grp_CS_svc_cluster_sps -sys cloud-svc-2
   ```

3. Restart if the status of all the SPS services is ONLINE.

```
[root@cloud-svc-1 ~] hagrp -offline Grp_CS_svc_cluster_sps -sys cloud-svc-1
```

4. Wait for SPS-1 status to go OFFLINE and run the following commands.

```
[root@cloud-svc-1 ~] virsh undefine sps
```

```
[root@cloud-svc-1 ~] hagrp -online Grp_CS_svc_cluster_sps -sys cloud-svc-1
```

5. Repeat step 3 and step 4 for the available SPSs.
6. Retry the credm command.
7. If at least SPS service status in an SVC node (in this example the nodes is the SVC-1) is FAULTED, restart it.

```
[root@cloud-svc-1 ~]# hagrp -state | grep FAULT
```

The system returns:

```
Grp_CS_svc_cluster_sps State cloud-svc-1 FAULTED
```

8. Fetch the complete SPS service name and run the following commands.

```
[root@cloud-svc-1 ~]# hagrp -clear Grp_CS_svc_cluster_sps
```

```
[root@cloud-svc-1 ~]# hagrp -online Grp_CS_svc_cluster_sps -sys cloud-svc-1
```

9. Wait for SPS on SVC-1 status switch to ONLINE and retry the credm command.

On cloud deployment:

10. Copy the key to the emp server using the private key for authentication. Log on emp server and list the consul members to view 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 ~]$ sudo su -
[root-user@ostk003-emp-0 ~]# consul members | grep sps
svc-1-sps               10.5.1.164:8301  alive   client  0.8.1  2         d →
c1
svc-2-sps               10.5.1.165:8301  alive   client  0.8.1  2         d →
c1
```

Verify that at least one instance of sps service is in alive state. If all instances are failed or left, wait for HA recovery. SAM finds the failure and triggers a HA workflow.

The service instance state moves from `failed` to `left` and then to `alive`.

For instances in `alive` state, restart each service.

```
> ssh -i <cloud-user private key> cloud-user@sps1
> sudo pkill consul
```

Results

The generic internal error is not raised after the execution of the `credm` command.

2.3 Service Entity Status Does Not Switch to `ACTIVE` after `credm reissue` Command

> This task resolves the issue after the execution of the `credm reissue` command.

Prerequisites

— A command window has been opened and the user has super user privileges.

See the *Connect to a Virtual Machine* section in ENM Troubleshooting Guide, Reference 19 for further information on how to connect to the VM.

Steps

1. Check the SPS service status on an SVC node.

   See the description in `credm` Command Returns an Internal Error on page 3.

2. Check the status of the `crond` service on the service VM (with root privilege).

   ```
   [root@svc-1-<service-name>]# service crond status
   ```

   If the current status of the `crond` service is `running`, the system returns:

   ```
   "crond (pid  NNNN) is running..."
   ```

   If the current status of the `crond` service is stopped, the system returns:

   ```
   "crond (pid  NNNN) is stopped..."
   ```

3. Start the `crond` service if it is not running.

   ```
   [root@svc-1-<service-name>]# service crond start
   ```

4. Check the following file.

   ```
   [root@svc-1-<service-name>]# cat /etc/cron.d/credentialmanagercli
   ```

   The file contains a string as in the example:

   ```
   <MM,mm>  * * * * root sh /opt/ericsson/ERICcredentialmanagercli/bin/credenti →
   almanagercliCrontab.sh   > /dev/null 2>&1
   ```

   Where *<MM,mm>* means that the `crond` service runs the CredentialManager process on this VM at minutes MM and mm of every hour (for example at *<hh:MM>* and *<hh:mm>*).

5. Check the log of previous CredentialManagerCLI runs located in:

   `/var/log/credentialmanager`

6. Check the certificate files used for the CredentialManagerCLI in:

   `/ericsson/credm/cli/data/certs`

7. Check the service certificates, if needed.

   See the description in Check Certificate and Trust Presence for a Service on page 29.

8. Check the following configuration file.

   Normally, it must have all the values commented with "#". It can be deleted.

   ```
   > cat /ericsson/tor/data/credm/conf/credentialManagerConfigurator.properties

   #memory_checker=false
   #forceCertificateRenewal=true
   ```

Results

The entity status of the service changes back to `ACTIVE` within 30 minutes.

3 ENM PKI Troubleshooting

> This section provides the troubleshooting steps recommended to diagnose and fix common problems in the ENM PKI Security service and in the Security Peer Server (SPS).

3.1 6001: Unrecognized CLI command `pkiadm` Error Message

If the connection between CmServ and SPS is not established properly, `pkiadm` commands are not available.

Prerequisites

No prerequisites.

Steps

1. Ensure that SPS Service is available.
    a. Log on the `svc-1` as `litp-admin`.
    b. Switch to root user.
    c. Verify the SPS service status.

    ```
    [root@cloud-svc-1~]# hagrp -state | grep sps
    ```

    If the SPS service status is `ONLINE`, the system returns as in the following example:

    Example

    ```
    Grp_CS_svc_cluster_sps          State                cloud-svc-1|O →
    NLINE|
    Grp_CS_svc_cluster_sps          State                cloud-svc-2|O →
    NLINE
    ```

    d. If the SPS service is not running on both `svc-1` and `svc-2`, switch the service to `ONLINE` for at least one VM (`svc-1` or `svc-2`):

    ```
    [root@cloud-svc-1~]# hagrp -online Grp_CS_svc_cluster_sps -sys clou →
    d-svc-1
    ```

    or

```
[root@cloud-svc-1~]# hagrp -online Grp_CS_svc_cluster_sps -sys clou →
d-svc-2
```

e. Verify the SPS service status.

```
[root@cloud-svc-1~]# hagrp -state | grep sps
```

If the SPS service status is `ONLINE` on one VM and `OFFLINE` to the other VM, the system returns as in the following example:

Example

```
Grp_CS_svc_cluster_sps          State                cloud-svc-1 | →
OFFLINE|
Grp_CS_svc_cluster_sps          State                cloud-svc-2 | →
ONLINE|
```

f. Switch the SPS service status to `ONLINE` on the offline VM.

```
[root@cloud-svc-1 ~]# hagrp -online Grp_CS_svc_cluster_sps -sys clo →
ud-svc-1
```

If the SPS service status on the other VM is also `ONLINE`, the system returns as in the following example:

Example

```
[root@cloud-svc-1 ~]# hagrp -state | grep sps
Grp_CS_svc_cluster_sps          State                cloud-svc-1 | →
ONLINE|
Grp_CS_svc_cluster_sps          State                cloud-svc-2 | →
ONLINE|
```

2. Connect to `CmServ`.
3. Go to the following directory:

   `/ericsson/3pp/jboss/`

4. Open `jboss-as.conf` file.
5. Check if *<REMOTE_EJB_HOSTS>* property contains `sps1,sps2` as shown in the example:

   Example

```
 REMOTE_EJB_HOSTS="medrouter1,medrouter2,mscm1,mscm2,sec1,sec2,fmserv1,fmser →
v2,impexp1,impexp2,shmserv1,shmserv2,sps1,sps2"
```

6. If the *<REMOTE_EJB_HOST>* property does not contain `sps1` and `sps2`, contact local Ericsson support.

Results

Connection between `CmServ` and SPS must be established properly.

3.2 "Unable to invoke the EJB" Error Message

A request of exporting profile or entity (download operation), or certificate generation causes this issue if a rpm has not been installed properly.

Prerequisites

No prerequisites.

Steps

1. Ensure that SPS Service is available.
    a. Log on the svc-1 as litp-admin.
    b. Switch to the root user.
    c. Verify the current SPS service status.

```
[root@cloud-svc-1~]# hagrp -state | grep sps
```

If the current SPS service status is `ONLINE`, the system returns an output as shown in the following example:

Example

```
Grp_CS_svc_cluster_sps          State                cloud-svc-1|O →
NLINE|
Grp_CS_svc_cluster_sps          State                cloud-svc-2|O →
NLINE
```

    d. Switch the service to `ONLINE` for at least one VM (svc-1 or svc-2), if the SPS service is not running on both svc-1 and svc-2.

```
[root@cloud-svc-1~]# hagrp -online Grp_CS_svc_cluster_sps -sys clou →
d-svc-1
```

or

```
[root@cloud-svc-1~]# hagrp -online Grp_CS_svc_cluster_sps -sys clou →
d-svc-2
```

    e. Verify the current SPS service status:

```
[root@cloud-svc-1~]# hagrp -state | grep sps
```

If the SPS service status is `ONLINE` on one VM and `OFFLINE` to the other VM, then the system returns an output as shown in the following example:

Example

```
Grp_CS_svc_cluster_sps          State                cloud-svc-1 | →
OFFLINE|
Grp_CS_svc_cluster_sps          State                cloud-svc-2 | →
ONLINE|
```

f. Switch the SPS service status to `ONLINE` on the other VM.

```
[root@cloud-svc-1 ~]# hagrp -online Grp_CS_svc_cluster_sps -sys clo →
ud-svc-1
```

If the SPS service status on the other VM is also `ONLINE`, then the system returns an output as shown in the following example:

Example

```
[root@cloud-svc-1 ~]# hagrp -state | grep sps
Grp_CS_svc_cluster_sps          State                cloud-svc-1 | →
ONLINE|
Grp_CS_svc_cluster_sps          State                cloud-svc-2 | →
ONLINE|
```

2. Log on db node.
3. Check if `ERICpkimanagerconfigmodel` RPM has been installed.

```
rpm qa | grep pkimanager-config-model
```

4. Enter the following command to install the RPM, if it has not been installed, otherwise go to the step 5:

```
rpm -ivh <rpm>
```

5. Do the following if RPM is installed:
    a. Log on sps server
    b. Open the `modelRepo.xml` file stored in:

    `/etc/opt/ericsson/ERICmodeldeployment/data/repo/modelRepo.xml`

    c. Check the presence of the `PkiWebCliExportCache` entry.
    d. Contact the support team if the `PkiWebCliExportCache` entry is not present.

Results

Profiles or entities are exported without errors.

3.3 PKI Error Code List

This section lists all the possible error codes for the pkiadm command set and the consequent actions while working with WEBCLI commands in the PKI system.

3.3.1 PKI System Configuration Error Codes

Error Code	Error Message	Example	Solution/Action Required
11001	Command syntax error	pkiadm cfg algo -list --type digest --enabled pkiadm cfg algo -l -t keygen -state disabled	See online help for correct syntax.
		pkiadm cfg algo -l -t keygenaration,digest -ks 512,2048	
		pkiadm cfg algo -l -n RSA -ks 1024-4096	
11006	An error occurred while executing the PKI command on the system. Consult the error and logs for more information. Could not find algorithms with name <algoritm-name>	pkiadm cfg algo --enable -n XYZAlgo	Specify an algorithm name which has been already configured in the system.

3.3.2 Profile Management Error Codes

Error Code	Error Message	Example	Solution/Action Required
6007	The file cert_profile.xml is not attached to command	pkiadm pfm -im -xf file:cert_profile.xml	A file must be associated with the command. Drag and drop a valid file into the CLI command area.
		pkiadm pfm -c -xf file:create_profile.xml	
		pkiadm pfm -c -xf file:create_profile.xml	
		pkiadm pfm -c -xf file:create_profile.xml	
11001	Command syntax error	pkiadm pfm -cb --xf cert_profile.xml	See online help for correct syntax.
		pkiadm profilemgmt --export -type certprofile -name certprof1	

Error Code	Error Message	Example	Solution/Action Required
11103	Error while deleting No profile found with name <certificate-name> No profile found : No profile found with Name: <certificate-name>	pkiadm pfm --delete --profiletype trust --name tp1	Trust Profile name must refer to a valid Trust Profile.
		pkiadm pfm --delete -type entity --name EP 1	Entity Profile name must refer to a valid Entity Profile.
		pkiadm profilemgmt --delete --profiletype certificate --name cert_prof1	Certificate Profile name must refer to a valid Certificate Profile.

3.3.3 PKI Entity Management Error Codes

Error Code	Error Message	Example	Solution/Action Required
11202	CAEntity not found with Name: CA1	pkiadm etm --delete --entitytype ca --name CA1	CA entity name must refer to a valid CA name.
6007	The file cert_profile.xml is not attached to command	pkiadm etm -im -xf file:entities.xml	A file must be associated with the command. Drag and drop a valid file into the CLI command area.
		pkiadm etm -c -xf file:entity_profile1.xml	
11001	Command syntax error	pkiadm etm -l -type ee -name EE1	Check online help for correct syntax.
		pkiadm entitymgmt --export -type endentiy -name ee1	
		pkiadm etm -cb --xf entities.xml	
		pkiadm etm --delete -type ee -name EE1	

3.3.4 PKI Certificate Management Error Codes

Error Code	Error Message	Example	Solution/Action Required
11001	Command syntax error	pkiadm ctm CACert -gen -ca ENMROOTCA	Check online help for correct syntax.
		pkiadm ctm CACert -ren -en ENMROOTCA -type regenerate	

Error Code	Error Message	Example	Solution/Action Required
		`pkiadm ctm CACert -l -en ENMROOTCA -s all`	Check user guide or online help for the list of the supported certificate status types.
11221	CA not found. Try with existing CA	`pkiadm ctm CACert -gen -en ENMROOTCA -f JKS -pass secure`	The entity with the given name does not exist in the system. Try with a valid entity.
11203	`Entity not Found, try with valid Entity`	`pkiadm ctm CACert -l -en ENMROOTCA -s active`	CA name must refer to a valid CA Entity.

3.3.5 PKI Entity Certificate Error Codes

Error Code	Error Message	Example	Solution/Action Required
6007	`The file cert_profile.xml is not attached to command`	`pkiadm ctm EECert --generate -entity REBS1234 -csr file:CSR.csr`	A file must be associated with the command. Drag and drop a valid file into the CLI command area.
		`pkiadm ctm EECert -gen -en RBS1234 -csr file:/var/tmp/CSR.csr`	
		`pkiadm ctm EECert -gen -en RBS1234 -crmf file:/var/tmp/CRMF`	
		`pkiadm ctm EECert -gen -en RBS1234 -crmf -csr file:CSR.csr`	
11001	`Command syntax error`	`pkiadm ctm EECert -l -en XYZ1234 -status active`	Check online help for correct syntax.

3.3.6 PKI Online Certificate Enrollment Using SCEP Error Codes

Error Code	Error Message	Example	Solution/Action Required
6001	`Unrecognized CLI command secadm`	`secadm certifcate issue -ct OAM -xf file:scep.xml`	Check the online help for valid ENM CLI commands.
6007	`The file scep.xml is not attached to command.`	`secadm certificate issue -ct OAM -xf file:scep.xml`	A file must be associated with the command. Drag and drop a valid file into the ENM CLI command area.
		`secadm certificate issue -ct OAM -xf file:/var/tmp/scep.xml`	
6008	`Invalid file name`	`secadm certificate issue -ct OAM -xf file:scepppp.xml`	File name has to the name of the file that is dragged in to ENM CLI command area. Specify a valid file name.

Error Code	Error Message	Example	Solution/Action Required
		`secadm certificate issue -ct OAM -xf file:/var/tmp/scepppp.xml`	

3.3.7 PKI Online Certificate Enrollment Using CMPv2 Error Codes

Error Code	Error Messages	Example	Solution/Action Required
6001	`Unrecognized CLI command secadm`	`secadm certifcate issue -ct OAM -xf file:CMP.xml`	Check the online help for valid ENM CLI commands.
6007	`The file CMP.xml is not attached to command`	`secadm certificate issue -ct OAM -xf file:CMP.xml` `secadm certificate issue -ct OAM -xf file:/var/tmp/CMP.xml`	A file must be associated with the command. Drag and drop a valid file into the ENM CLI command area.
6008	`Invalid file name`	`secadm certificate issue -ct OAM -xf file:CMPv2.xml` `secadm certificate issue -ct OAM -xf file:/var/tmp/CMPv2.xml`	File name has to be the name of the file that is dragged in to ENM CLI command area. Specify a valid file name.

3.3.8 PKI Revocation Management Error Codes

Table 1

Error Code	Error Message	Example	Solution/Action Required
11001	`Command syntax error`	`pkiadm revmgmt CA --revk --entityname ENMSUBCA --reasontext unspecified`	Check the online help for correct syntax.
11202	`CRL(s) publishing failed for ENMPKIABCCA Please check the logs for more information.`	`pkiadm crlmgmt --publish --caentityname ENMPKIABCCA`	Check the logs for more information.
	`Certificate revocation failed. Entity name may be incorrect. Please check the logs for more information.`	`pkiadm revmgmt CA --revoke --entityname ENMSUBCAABC --reasontext unspecified --invaliditydate "2014-11-21 23:11:10"`	
11601	`Revocation Reason not supported`	`pkiadm revmgmt CA --revoke --entityname ENMROOTCA --reasontext unspecifieded`	Check the online help for the list of the supported revocation reason value.

Error Code	Error Message	Example	Solution/Action Required
11602	Root CA cannot be revoked.	pkiadm revmgmt CA --revoke --entityname <<RootCA Name>> --reasontext unspecified	Enter the RootCA name for revocation.
11603	Certificate is expired	pkiadm revmgmt CA --revoke --entityname ENMROOTCA123 --reasontext unspecified	Use valid Certificate for operation.
11323	Certificate not found for the entity.	pkiadm revmgmt EE --revoke --entityname ERBS123 --reasontext unspecified	Use valid Certificate for operation.
11604	Invalid Certificate chain. One of the certificates in chain is revoked. Certificate serial number: 452c6ae410c67f57 and Certificate subject: CN=ARJ_Root	pkiadm revmgmt EE --revoke --issuername ERBS123 --serialno 452c6ae410c67f57 --reasontext unspecified --invaliditydate "2016-11-21 23:11:10"	Issuer Certificate must be valid to revoke Entity Certificate.
11606	Issuer is not found, Please refer to an existing issuer.	pkiadm revmgmt CA --revoke --issuername ENMPKIROOTCAXYZ --serialno 5f5b76b3d4792483 --reasontext unspecified --invaliditydate "2014-11-21 23:11:10"	Refer to an existing issuer.
11607	Invalid argument: Date format error.Supported Format is yyyy-MM-dd HH:mm:ss.	pkiadm revmgmt CA --revoke --entityname ENMXYZCA --reasontext unspecified --invaliditydate "2014/11/21 23:11:10"	Supported Format is yyyy-MM-dd HH:mm:ss
11608	CRL $OPERATORACTION(gereration,download,listing) failed.T he CA entity name or CA Certificate Serial Number is incorrect.	pkiadm crlmgmt --generate --caentityname ENMPKIABCCA --serialno 1cg4f7	Check the logs for more information.
11609	CRL generation failed.The CRL can not be generated for the CA Certificate Status EXPIRED Allowed CA Certificate statues are ACTIVE and INACTIVE. Please check user guide or online help for command syntax.	pkiadm crlmgmt --generate --caentityname ENMPKIROOTCA --status expired	Allowed CA Certificate statues are "ACTIVE" and "IN ACTIVE". Check the user guide or online help for command syntax.
11610	CRL generation failed for NEOAMCA, ENMPKIROOTCA, ENMOAMCA.An error occurred while executing the PKI command on the system. Consult the error and logs for more information.	pkiadm crlmgmt --generate --caentityname ENMPKIABCCA,ENMPAMCA,NETAMCA --status inactive	Check the logs for more information.
11302	The CRL can not be downloaded for the CA Certificate Status inactive1 Certificate status not supported. Supported	pkiadm crlmgmt --download --caentityname ENMROOTCA --status inactive1	Allowed CA Certificate statues are "ACTIVE" ,"INACTIVE","EXPIRED" and "REVOKED". Check user guide or online help for command syntax.

Error Code	Error Message	Example	Solution/Action Required
	values are [active,revoked,expired]		

3.3.9 PKI Trust Distribution Point Service Error Codes

Error Code	Error Message	Example	Solution/Action Required
11001	Command syntax error	pkiadm tsm --publish -name ENM_CA	See the online help for correct syntax.
11202	No Entity found with given name. Please refer an existing entity and try again.	pkiadm trustmgmt --list --entitytype ee --entityname ENMInfrastructureCA12	See the logs for more information.
11203	Invalid argument value: Entity doesn't exist	pkiadm trustmgmt --list --entitytype ca --entityname ENMInfrastructureCA12	See the logs for more information.
11321	Certificates with the given CA entity Name not found	pkiadm trustmgmt --publish --entitytype ca --entityname svc-1	See the logs for more information.
	Certificates with the given End entity Name not found	pkiadm trustmgmt --publish --entitytype ee --entityname svc-1	

3.4 Enrollment for Baseband RadioNode Fails Due to the SERIALNUMBER Attribute in the Certificate

Initial enrollment using CMP protocol fails on Baseband RadioNode as the ENM PKI system contains SerialNumber attribute in the **Subject DN** field of CA and Entity Certificates.

This is because of the limitation on the node that it does not support SerialNumber attribute in the **Subject DN** field.

This workaround removes the `Serial Number` attribute from the `SubjectDN` of certain CA certificates of ENM PKI system.

Prerequisites

— PKI Administrator role.

Steps

1. Disable `CredM` checks.

   Refer to step 1 of *Disable CredM Checks During Certs and Trusts Distribution Procedure* section of the document ENM Public Key Infrastructure System Administrator Guide, [22] to complete this step.

2. Remove the `Serial Number` attribute from the following CA entities.
   - NE_OAM_CA
   - NE_IPsec_CA

   Run the following to remove the `Serial Number` attribute:

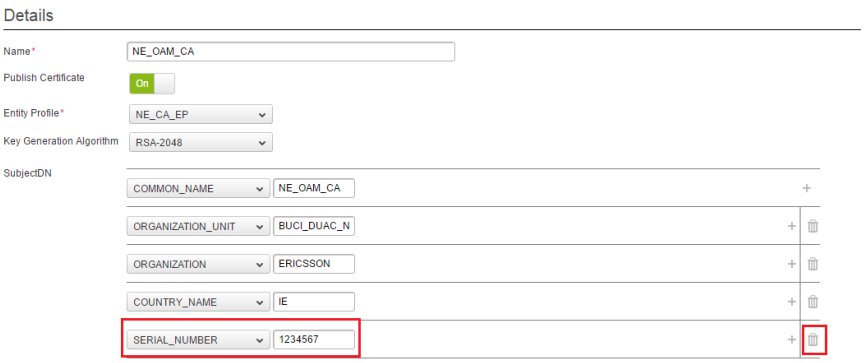
   a. Open **PKI Entity Management** User Interface.

   b. Select the **CA** from the list of CAs and click **Edit**.

   c. Scroll down to the attribute `SubjectDN` and click the delete icon beside the `Serial Number` attribute.

   d. Save the Entity.

   Example



3. Reissue all the CAs of the `ENM PKI` system in the following order:
   a. ENM_PKI_Root_CA
   b. ENM_Infrastructure_CA
   c. ENM_OAM_CA
   d. ENM_Management_CA
   e. ENM_UI_CA
   f. ENM_NBI_CA
   g. ENM_E-mail_CA
   h. ENM_External_Entity_CA
   i. NE_External_CA
   j. NE_IPsec_CA
   k. NE_OAM_CA

Reissue CAs using the following command:

```
pkiadm certmgmt CACert --reissue --entityname <name of CA> --reissuetype ren →
ew --level CA
```

4. Verify that the following CA certificates do not contain the `Serial Number` attribute in the `Subject` field:

   — NE_IPsec_CA

   — NE_OAM_CA

      a. Run the following command to verify the CA certificate:

```
pkiadm ctm CACert &8211;l &8211;en  <CA Entity Name>
```

Example

```
»pkiadm ctm CACert -l -en NE_OAM_CA
List of Certificate(s)
Entity Name   Subject                                          Status   Issuer                                                  Serial Number
NE_OAM_CA     OU=BUCI_DUAC_NAM, O=ERICSSON, C=SE, CN=NE_OAM_CA ACTIVE   OU=BUCI_DUAC_NAM, O=ERICSSON, C=SE, CN=ENM_PKI_Root_CA  3695ba4236025312

Command Executed Successfully
```

5. Redistribute the trusted certificates to the Network Elements.

      a. Retrieve the Trust certificate state using ENM CLI command:

```
secadm trust get -ct <IPSec|OAM> -n <Node Name>
```

Example

```
»secadm trust get -ct OAM -n LTE01ERBS00001
Node Name                          Install State  Install Error Message  Subject                                                                  Serial Number
NetworkElement=LTE01ERBS00001      IDLE           Not Applicable         C=SE, O=Ericsson, OU=EAB, CN=CPP Ericsson1 Root Certificate Authority   0
```

      b. Distribute trusts to nodes using ENM CLI command:

```
secadm trust distr -ct <IPSEC|OAM> -nf file:<file name>
```

6. Lock and unlock all Service Blades.

   See the step 3 of *Disable CredM Checks During Certs and Trusts Distribution Procedure* of the document ENM Public Key Infrastructure System Administrator Guide, [22] to complete this step.

7. Reissue certificate for `haproxy-ext`.

   See the step 4 of *Disable CredM Checks During Certs and Trusts Distribution Procedure* of the document ENM Public Key Infrastructure System Administrator Guide, [22] to complete this step.

8. Re-enable CredM checks.

See the step 5 of *Disable CredM Checks During Certs and Trusts Distribution Procedure* of the document ENM Public Key Infrastructure System Administrator Guide, [22] to complete this step.

9. Update the node configuration by updating the `enrollmentAuthorityName` and `enrollmentCaFingerprint` attributes in *<SystemFunctions=1>*,*<SecM=1>*,*<CertM=1>*,*<EnrollmentAuthority MO>*.

10. Perform the enrollment and verify that it is successful.

3.5 IPsec Certificate Enrollment Fails for RadioNode

CMP Enrollment using IPsec mode (or profile) fails for Radio Node during auto integration.

This is because the `issuer_id` value is null in certificate table for external ca.

The workaround sets the `issuer_id` value in certificate table of certain external CA certificates of ENM PKI system.

Prerequisites

— User must have PKI Administrator role.

Steps

1. List the external CA certificates using ENM CLI command.

   Example

```
»pkiadm extcalist
 List of Certificate(s)
 External CA Name                                    Subject                                             Issuer
 CN=ExternalRootCA, O=TCS, L=Hyd, ST=Telangana, C=IN CN=ExternalRootCA, O=TCS, L=Hyd, ST=Telangana, C=IN CN=ExternalRootCA, O=TCS, L=Hyd, ST=Telang
 CN=ExternalIntermediateCA, O=TCS, ST=Telangana, C=IN CN=ExternalIntermediateCA, O=TCS, ST=Telangana, C=IN CN=ExternalRootCA, O=TCS, L=Hyd, ST=Telang
 VC_Root_CA_A1                                       CN=VC_Root_CA_A1, O=Ericsson, C=SE                  CN=VC_Root_CA_A1, O=Ericsson, C=SE

 Command Executed Successfully
```

2. Connect to `pkimanagerdb`:

```
/opt/rh/postgresql92/root/usr/bin/psql -U postgres -d pkimanagerdb
```

3. Compare the subject and issuer value from step 1 for each CA.

   If the subject and issuer match execute the `sql` commands.

   a. Select id from `caentity` where name is *<External CA Name>*.

      Example

      select id from `caentity` where `name` = *<CN=ExternalRootCA>*, O= *<TCS>*, L= *<Hyd>*, ST= *<Telangana>*, C= *<IN>*.

```
pkimanagerdb=# select id from caentity where name ='CN=ExternalRootCA, O=TCS, L=Hyd, ST=Telangana, C=IN';
 id
----
 23
(1 row)
```

b. Select `certificate_id` from `ca_certificate` where `ca_id` =*<provide id value* as result of previous SQLcommand.

Example

```
pkimanagerdb=# select certificate_id from ca_certificate where ca_id=23;
 certificate_id
----------------
             66
(1 row)
```

c. Select `issuer_id` from certificate where `id` =*< id value>* result of previous SQL command.

d. Check the output if `issuer_id` is null execute step e.

Example

```
pkimanagerdb=# select issuer_id from certificate where id=66;
 issuer_id
-----------

(0 row)
```

e. Update the certificate set `issuer_id` =*<id value>* result of previous SQL command a, where `id` =*< id value>* result of previous SQL command b.

Example

```
pkimanagerdb=# update certificate set issuer_id=23 where id=66;
UPDATE 1
```

4. Compare the subject and issuer value from above step 1 for each CA.

a. Execute the SQL commands, if subject and issuer differ.

Select id from `caentity` where name =*<external ca name>*;

<external ca name> takes the name as returned from ENM CLI command `pkiadm extcalist`.

Example

```
pkimanagerdb=# select id from caentity where name ='CN=ExternalIntermediateCA, O=TCS, L=Hyd, ST=Telangana, C=IN';
 id
----
 24
(1 row)
```

b. Select `certificate_id` from `ca_certificate` where `ca_id` =*< id value>* result of previous SQL command.

Example

```
pkimanagerdb=# select certificate_id from ca_certificate where ca_id=24;
 certificate_id
----------------
             67
(1 row)
```

c. Select `issuer_id` from certificate where `id =<id value>` result of previous SQL command b.

d. Check if `issuer_id` value is null then execute step e.

Example

```
pkimanagerdb=# select issuer_id from certificate where id=67;
 issuer_id
-----------

(0 row)
```

e. Update certificate set `issuer_id = <issuer_id>` value, result of previous `sql` command a of step 3, where `id =< id value>` result, of previous `sql` command b.

provide `issuer_id` result, of previous `sql` command a, from Step 3.

In this example, for external CA is `CN=<ExternalIntermediateCA>`, `O=<TCS>`, `L=<Hyd>`, `ST=<Telangana>`, `C=<IN>` and issuer is `CN=<ExternalRootCA>`, `O=<TCS>`, `L=<Hyd>`, `ST=<Telangana>`, `C=I<N>` `issuer_id` to be set as 23.

Example

```
pkimanagerdb=# update certificate set issuer_id=23 where id=67;
UPDATE 1
```

5. Perform the enrollment and verify that it is successful.

Results

Enrollment is successful.

3.6 Remove Subject-DN Extra Attributes from ENM System

The Subject Distinguished Name (Subject DN) field identifies the entity associated with the public key stored in the subject public key field. The Subject DN is made up of multiple Relative Distinguished Names (RDNs). The Subject DN is an ordered sequence of RDNs, and each RDN is an unordered set of Attribute Value Assertion (AVA). An AVA refers to "CN=somename" or "O=Ericsson". Standard sets of attributes have been defined in the X.500 series of specification. The supported attributes in ENM PKI system are:

— COMMON_NAME

— SURNAME

— COUNTRY_NAME

— LOCALITY_NAME

— STREET_ADDRESS

— STATE

— ORGANIZATION_UNIT

— ORGANIZATION

— DN_QUALIFIER

— TITLE

— GIVEN_NAME

— SERIAL_NUMBER

However, all the previous attributes are not supported by all the network elements. To avoid the occurrence of an exception during an enrollment and post sync because of unsupported attributes, only the following attributes must be retained:

— COMMON_NAME

— COUNTRY_NAME

— ORGANIZATION_UNIT

— ORGANIZATION

The extra Subject DN attributes must be removed from all ENM PKI CA Entities and End Entities (Both Nodes and ENM Services). The extra attributes are:

— SURNAME

— LOCALITY_NAME

— STREET_ADDRESS

— STATE

— DN_QUALIFIER

— TITLE

— GIVEN_NAME

— SERIAL_NUMBER

Note:
- To remove the extra attributes from CA and End Entity certificates, they must be reissued.
- Performing the end- to-end procedure takes considerable amount of time as it requires a systematic restart of all the service blades. Considering 20 minutes per blade to restart for a four blade server, it takes up to two hours.

3.6.1 Remove Subject DN Extra Attributes from ENM PKI CA and Entity Certificates

> Use this procedure to remove extra `subjectDN` attributes from CA and Entity certificates.

Prerequisites

- Access with the following roles:
  - PKI Administrator
  - NodeSecurity Administrator
  - `Credm` Administrator
- Root privilege to ENM deployment server.

Steps

1. Disable automatic CredM Checks.

   The credential manager `cron` job must be disabled before reissuing the CA certificates. Execute Step 1 of the procedure *Disable CredM Checks during Certs and Trusts Distribution Procedure* section of the document ENM Public Key Infrastructure System Administrator Guide, [22].

2. List and edit Entity Profiles of CA, nodes, and ENM services.

   To list all the Entity Profiles that are available in the system, do the following steps. After entering the command on the ENM CLI, press **CTRL+ENTER** and provide a file name to export the output to a file.

   ```
   pkiadm profilemgmt --list --profiletype entity
   ```

   OR

   ```
   pkiadm pfm -l --profiletype entity
   ```

3. Unlock Entity Profiles.

By default, the Entity profiles are locked and not modifiable. To edit the profiles, operator must unlock them and edit to remove the extra parameters. All the profiles that are obtained using step 2 must be unlocked and modified using step 4.

Refer to the *Lock and Unlock Certificate and Entity Profiles* section of the document ENM Public Key Infrastructure System Administrator Guide, [22].

4. Edit an Entity Profile.

    a. Open **PKI Profile Management** UI and filter on Entity Profile to display only Entity Profiles to unlock each entity profile that needs to be edited.

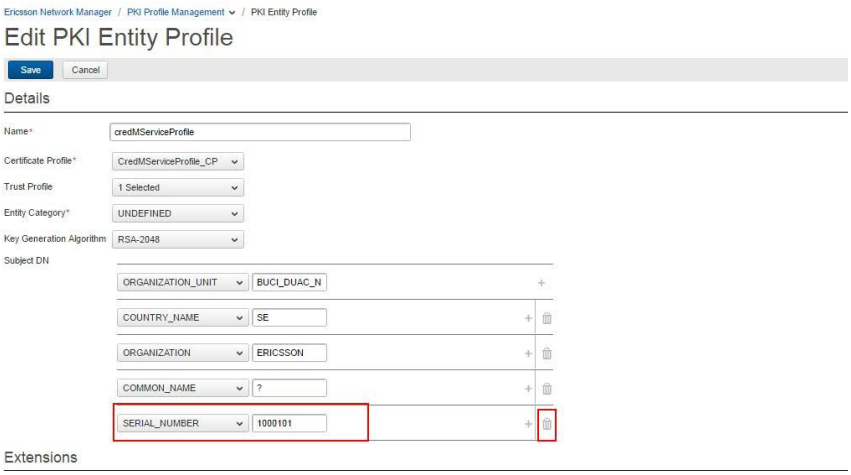
    b. Select the entity profile from the list of entity profiles and select **Edit**.

    c. Scroll down to the option `SubjectDN` and use delete icon to delete all the extra attributes.

    d. Select **Save** to save the entity profile.

    Example

    The following example illustrates how to delete Serial Number attribute from entity profile credMServiceProfile. Similarly, all the extra attributes can be removed from all the entity profiles.



5. Lock Entity Profiles.

    to unlock each entityAfter the entity profiles that have been unlocked in step 3 and successfully edited, must be locked again. See the *Lock and Unlock Certificate and Entity Profiles* section of the document ENM Public Key Infrastructure System Administrator Guide, [22] to lock the profiles.

6. Edit CA Entities.

    Access the PKI Entity Management UI to edit the CA entities. The following CA entities are updated:

- ENM_PKI_Root_CA
- ENM_Infrastructure_CA
- ENM_OAM_CA
- ENM_Management_CA
- ENM_UI_CA
- ENM_NBI_CA
- ENM_E-mail_CA
- ENM_External_Entity_CA
- NE_External_CA
- NE_IPsec_CA
- NE_OAM_CA

7. Update an Entity

   Perform the following to edit and save all the CA entities and delete extra attributes.

   a. Open PKI Entity Management UI.

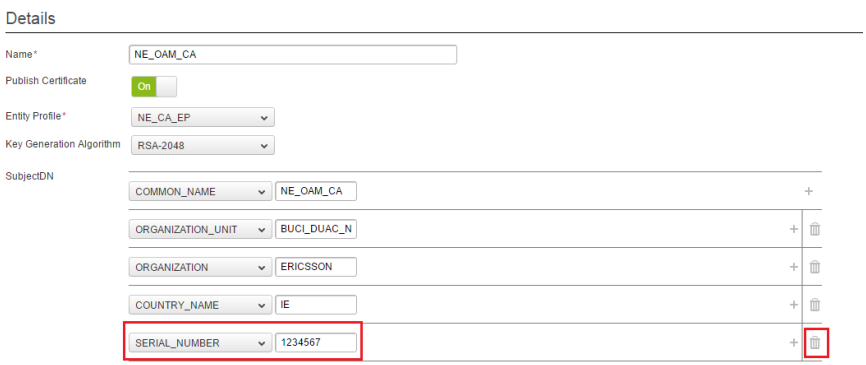
   b. Select the entity from the list of entities and select **Edit**.

   c. Scroll down to the option SubjectDN and use **delete** icon to delete all the extra attributes.

   d. Select **Save** to save the entity.

      Example

      The following example explains how to delete Serial Number attribute from entity `NE_OAM_CA`. Similarly, all the extra attributes can be removed from any CA entity.



8. Reissue the CA Entity Certificates and generate CRLs.

   To remove the extra attributes from subject DN, reissue all the CA entity certificates.

   Steps to reissue all CA entity Certificates.

   a. Open **PKI Entity Management** UI.

   b. Select the entity `ENM_PKI_Root_CA` from the list of entities.

   c. Select the **Reissue** option.

   d. Select **Include full CA chain** check box and select the reissue type, `CA_WITH_ALL_CHILD_CAS`.

   e. Select and confirm **Reissue** to reissue all the CA entity certificates.

      Example

      The following example illustrates how to choose the options to reissue the ENM_PKI_Root_CA.

   f. Generate CRLs using ENM CLI command for the CAs that have been reissued.

```
pkiadm crlmgmt --generate --caentityname <Name of CA> --status acti →
ve
```

9. Publish Certificates to TDPS.

   Publish CA Certificates to TDPS using ENM CLI command.

   ```
   pkiadm trustmgmt --publish --entitytype ca --entityname <Name of CA>
   ```

10. Distribute Trusted Certificates

    Redistribute trusts to the Network Elements. See the *Distribute Trust Certificates to a Node* section of the document ENM Public Key Infrastructure System Administrator Guide, [22].

    As part of IPsec setup, trusted certificates are installed on Security Gateway for authentication.

    For trust distribution on Security Gateway, perform the procedure *Trust Distribution for Security Gateway* of the document ENM Public Key Infrastructure System Administrator Guide, [22].

11. Perform lock and unlock to Restart Services.

    Run the steps 3, 4, and 5 of the *Disable CredM Checks during Certs and Trusts Distribution Procedure* section of the document ENM Public Key Infrastructure System Administrator Guide, [22] to complete the step.

    Perform lock and unlock operations for the service blades. It restarts the services in a systematic way to reissue certificates and trusts to the ENM subsystems.

12. Reissue All Node Certificates.

    ```
    secadm certificate issue -ct <IPSEC|OAM> -xf file:<file name>
    ```

    See the online help to reissue node certificates with various available options.

    Provide new certificate to SecGW with CSR following the procedure *Offline Enrollment on Security Gateway with CSR* of the document ENM Public Key Infrastructure System Administrator Guide, [22].

    Provide new certificate to SecGW without CSR following the procedure mentioned in *Offline Enrollment on Security Gateway without CSR* of the document ENM Public Key Infrastructure System Administrator Guide, [22].

13. Remove old Trusts from nodes.

    Remove old trust certificates from the node using ENM CLI after the new trust has been distributed and node certificates have been reissued.

    ```
    secadm trust remove -ct <IPSec|OAM> --issuer-dn "<issuer_name>" -sn <ca seri →
    alnumber> -n Node_Name
    ```

14. Revoke Inactive CA Certificates

    Revoke the inactive CA certificates in the following order:

    a. ENM_NBI_CA

    b. ENM_UI_CA

    c. ENM_Management_CA

    d. ENM_OAM_CA

    e. NE_OAM_CA

    f. NE_IPsec_CA

    g. NE_External_CA

    h. ENM_External_Entity_CA

    i. ENM_E-mail_CA

    j. ENM_Infrastructure_CA

```
pkiadm revmgmt CA --revoke --issuername <<issuer name>> --serialno <<serial
number>> --reasontext unspecified --invaliditydate <<invalidity date>>
```

Note: Revoking inactive CA Certificates is optional and can result in restart of some ENM services.

4 Check Certificate and Trust Presence for a Service

This task checks certificate and trust presence for a service.

Prerequisites

— A command window has been opened and the user has super user privileges.

  See the *Connect to a Virtual Machine* section in the document ENM Troubleshooting Guide, Reference [19] for further information how to connect to the required VM.

Steps

1. See the instructions on Connect to a Virtual Machine to log on the service VM.
2. Search for CredentialManagerCLI certificates in:

   `/ericsson/credm/cli/data/certs`

   and check if certificate and `truststore` files are present:

   ```
   $ ls
   credmApiKS.JKS  credmApiTS.JKS
   ```

3. Search if at least one XML file is present in the path.

   `/ericsson/credm/data/xmlfiles`

   The Credential Manager uses these XML files to check the validity of the needed certificates and trusts and to generate them if required.

4. Extract from the XML files the `keystore` info.

   Search for the *<keystore>* tag to read the values of the *<storelocation>* tag (filename with complete path is expected) as in the example:

   Example

   ```
   <storelocation>/ericsson/credm/data/certs/Certificate.JKS</storelocation>)
   ```

5. Search for the certificate file indicated by *<storelocation>* as in the example:

   Example

   ```
   ls -la <file_with_path>
   ```

6. Extract from the XML files the truststore info.

   Search for the *<truststore>* tag to read the values of the *<<storelocation>>* tag (filename with complete path is expected) as in the following example:

   Example

   ```
   <storelocation>/ericsson/credm/data/certs/Trust.JKS</storelocation>
   ```

7. Search for the trust file indicated by *<storelocation>* as in the example:

   Example

   ```
   ls -la <file_with_path>
   ```

5 Enable Default Administrator User

> This task describes how a root user with security administrator privileges who loses access to **ENM Launcher** and **User Management** applications can retrieve it, by executing script to enable the default user "administrator".

The script can only be launched from Management Server (ms-1) and can be found in the following directory:

`/opt/ericsson/openidm/enable_admin_user.sh`

Note: This task is only valid for an ENM on physical deployment.

Prerequisites

— User has root access to db node.

Steps

1. Use `cd` command to directory and run the script to change default administrator status, log on ms-1.

   ```
   cd /opt/ericsson/openidm/sh enable_admin_user.sh
   ```

2. Type 'Yes' if the following output appears:

   ```
   The authenticity of host 'openidm (**IP_adress**)' can't be established.
   RSA key fingerprint is *******.
   Are you sure you want to continue connecting (yes/no)?
   ```

3. Enter password for required node.

   ```
   litp-admin@db-1's password:
   ```

Results

After the steps are completed, the following output is displayed upon successful completion of the command and user is able to use **ENM Launcher**:`Done . Administrator user is now ENABLED.`

6 Troubleshooting Node Security Issues

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

6.1 Troubleshooting on Create and Update Node Credentials

> This section provides the troubleshooting steps recommended to diagnose and fix common problems in while creating or updating node credentials using the secadm credentials ENM CLI commands.

Further information can be retrieved on ENM CLI online help.

```
»secadm help
```

If root cause is not identified, collect logs of the secserv VMs. See the *If Issue Suspected on Node Security* section of ENM Data Collection Guide for further information on how to connect to the required secserv VM.

Prerequisites

Steps

The credentials (username and password) allowed when creating or updating node credentials depend on the node types of involved nodes.

1. Ensure that only valid credentials for the involved node types are specified. See ENM CLI online help for more details.

The create credentials are performed on nodes that do not have credentials created.

2. Read the current node credentials status for a node using the following ENM CLI commands:

   ```
   »secadm credentials get --nodelist <node-name>
   ```

   or

   ```
   »cmedit get <node-name> NetworkElementSecurity.*
   ```

The update credentials are performed on nodes that already have credentials created.

3. Read the current node credentials status for a node using the following ENM CLI commands:

```
»secadm credentials get --nodelist <node-name>
```

or

```
»cmedit get <node-name> NetworkElementSecurity.*
```

6.2 Troubleshooting on Issue and Reissue a Node Certificate

> This section provides the troubleshooting steps recommended to diagnose and fix common problems in while issue or reissue node certificate.

This section provides the troubleshooting steps recommended to diagnose and fix common problems while issuing or reissuing node certificates using the `secadm certificate` ENM CLI commands.

Further information can be retrieved by ENM CLI online help available by running the following ENM CLI command:

```
»secadm help
```

If root cause is not identified, collect logs of the `secserv`, `sps`, `pkiraserv`, `mscm` (if CPP nodes involved), and `mscmce` (if COM/ECIM nodes involved) VMs. See the *If Issue Suspected on Node Security* section of ENM Data Collection Guide, for further information on how to connect to the required `secserv`, `sps`, `pkiraserv`, `mscm` (if required), and `mscmce` (if required) VM.

Prerequisites

Steps

1. If the job finishes with an error, for each Workflow Status that does not have SUCCESS status:

    a. If Workflow Details signals a [TIMEOUT] condition:

    Example

    For CPP node types (`ERBS`, `RNC`, `RBS`, `MGW`)

    Verify that alarm supervision is enabled for that node: if it is disabled, check if, despite the workflow failure, the new certificate

was enrolled and issued to the node by reading the node certificate status.

Example

For COM/ECIM nodes

Verify that the error was not caused by a misalignment between node MOs and correspondent DPS MOs: force a resync operation on node and, when the node is synchronized again, read the node trusted certificates status to check that despite the workflow failure, the specified trusted certificates were enrolled and issued to the node.

On the ENM CLI: Read the nodeCredential attribute of `NetconfTls` MO of the node to get the FDN of referenced `NodeCredential` MO:

```
```

Read the referenced NodeCredential MO:»cmedit get <node-name> NetconfTls.nodeCredential

```
»cmedit get <nodeCredential FDN>
```

If the attribute renewalMode of the involved `NodeCredential` MO is MANUAL, set it to AUTOMATIC

```
»cmedit set <nodeCredential FDN> renewalMode=AUTOMATIC
```

Note:

If the certificate issue command is triggered with `extca` option and the workflow failed with TIMEOUT error, contact External CA to find more information on failure.

If the certificate reissue command is triggered for the node having External CA certificate and the workflow failed with TIMEOUT error, contact External CA to find more information on failure.

b. If Workflow Details signals an`»cmedit get [ERROR]` condition:

Example

`MGW`

For `MGW` node types, failure can be caused by a known node behavior: the node restarts after installing a new certificate (so causing workflow to fail). Check if, despite the workflow failure, the new certificate was enrolled and issued to the node by reading (when the node is synchronized again) the node certificate status.

Example

`MSRBS_V1 (pico)`

For `MSRBS_V1 (pico)` node types this failure can be caused by a known node behavior: the node restarts after installing a new certificate (so causing workflow to fail). Check if, despite the workflow failure, the new certificate was enrolled and issued to the node by reading (when the node is synchronized again) the node certificate status. If, despite the workflow failure, the new certificate was enrolled and issued to the node, apply following steps from ENM CLI:

read the nodeCredential attribute of `NetconfTls` MO of the node to get the FDN of referenced `NodeCredential` MO:

```
»cmedit get <node-name> NetconfTls.nodeCredentia
```

Read the referenced `NodeCredential` MO:

```
»cmedit get <nodeCredential FDN>
```

If the attribute renewalMode of the involved `NodeCredential` MO is `MANUAL`, set it to `AUTOMATIC`:

```
»cmedit set <nodeCredential FDN> renewalMode=AUTOMATIC
```

c. If Workflow Details signals a `[FAILURE]` condition:

Read the node certificate status, the Enroll Error Message can provide some useful information about the root cause of failure detected on node side.

If no useful information is evident, the analysis focuses on the node side as the node is explicitly signaling a failure detected on its side.

2. This could be caused by a misalignment between node MOs and correspondent DPS MOs: force a `resync` operation on node and read the node certificate status to verify that the new certificate is read (new value in Serial Number):

```
cmedit action NetworkElement=<node-name>,CmFunction=1 sync --force
```

3. Check for the following points if the certificate issue use case is failed with the error as shown in the following example.If job finishes with success but the node certificate status indicates that the old certificate is read (old value in Serial Number):

Example

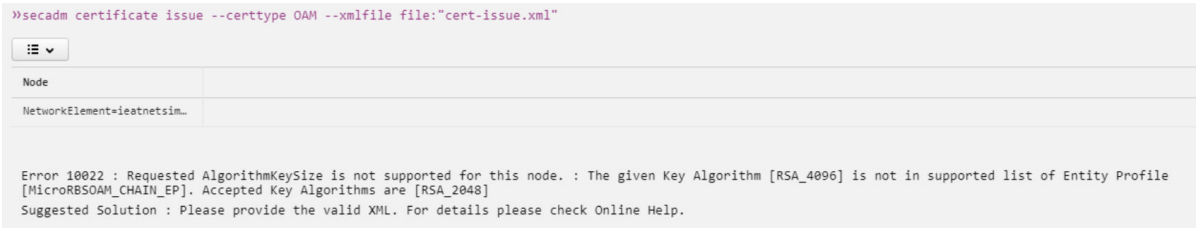


Figure 1

— Check whether the desired Key Size is present in the **Supported KeySize** values of the respective node type in **secadm certificate issue** online help.

  - If not Supported, then desired `Key Size` is not valid and use case cannot be performed with that `Key Size`.
  - If job finishes with success but the node certificate status indicates that theIf Supported, then follow the next steps to enable it in the associated Entity Profile.

— To Enable the desired Key Size in Entity Profile, the same should be added to the Certificate Profile which is referred in the respective Entity Profile.

  a. Launch **ENM CLI**.

  b. Unlock the Certificate Profile that needs to be updated using the following command.

  ```
  credm unlock --profile <certificate-profile-name> --type certificate
  ```

  c. Launch **PKI Profile Management** from **ENM Launcher**, select the **Certificate Profile** that needs to be updated and add the required algorithm with key size in **Key Generation Algorithm** field as shown in the following example.

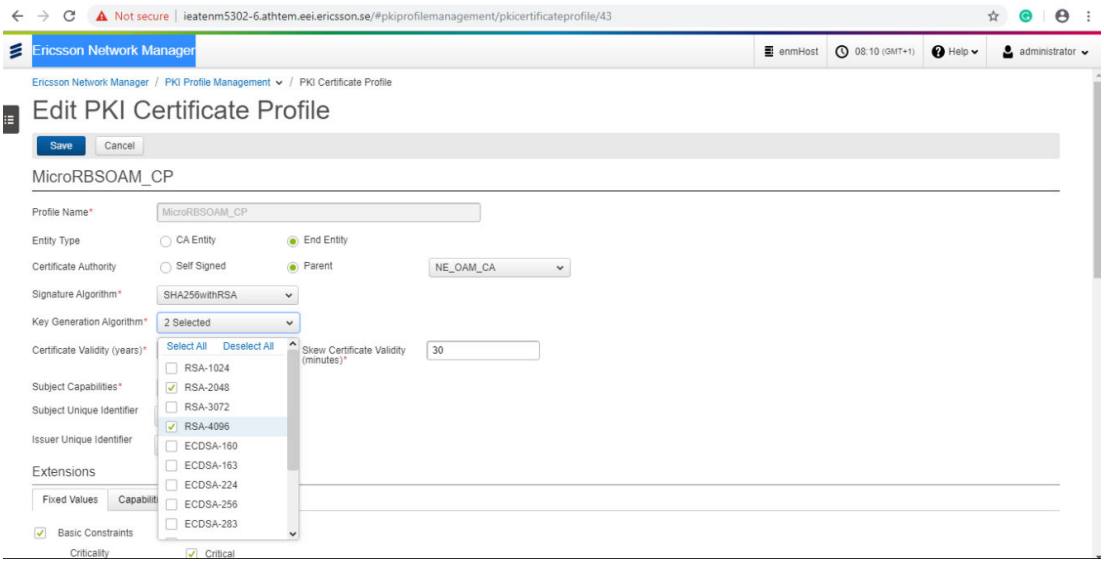


Figure 2

d. Save the **Certificate Profile** after adding the desired **Key Generation Algorithm** with key size as mentioned in the previous step.

e. In **ENM CLI**, unlock the Entity Profile that needs to be updated using the following command.

```
credm unlock --profile <entity-profile-name> --type entity
```

f. In **PKI Profile Management**, select the **Entity Profile** which was mentioned in the error, edit the profile and check for the Key Generation Algorithm with desired key size presence in Key Generation Algorithm field in Entity Profile as shown in Example. Save the Entity Profile.

Example:

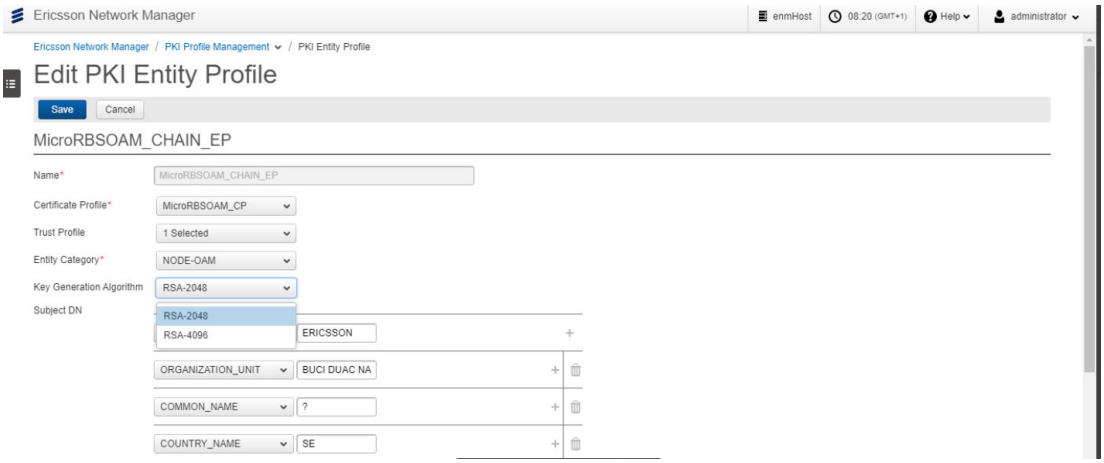


Figure 3

In the example, RSA_4096 in Entity Profile has been added successfully.

g. Certificate Issue use case must be performed after performing the previous steps. Then the use case is executed successfully.

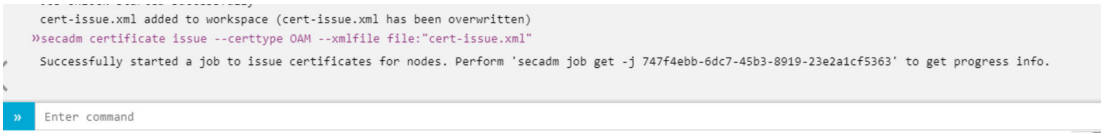


Figure 4

Results

The issue/reissue node trusted certificates command is asynchronously managed:

A job is created (uniquely identified by a *<job-id>*) and a set of associated workflows is scheduled (one workflow for each valid node).

A response, containing the *< <job-id>>* and the list of specific errors for invalid nodes, is returned to the user.

Asynchronously, each workflow is executed to perform the requested operations on node:

for CPP node types (ERBS, RNC, RBS, MGW), the workflow generally performs actions on node and the action progress result is available to workflow through events sent by node itself,

for COM/ECIM node types, the workflow performs actions on node and the action progress result is available through an active poll performed by workflow itself reading specific node objects.

The user can monitor the progress of the job (and of related workflows) using the following ENM CLI command:

```
»secadm job get -j <job-id>
```

The response contains an overall Job Status and a Workflow Status for each workflow.

The job finishes when Job Status is set to COMPLETED.

The final status of each workflow is then available in Workflow Status:

— if it is set to SUCCESS, the requested operations on that node were successful

— if it is set to RROR, the requested operations on that node failed: the user can retrieve more information on the failure from the Workflow Details:

— it contains [TIMEOUT] when an action performed on the node did not complete within maximum expected time

— it contains [FAILURE] when the node itself explicitly signaled a failure in the execution of an action

— it contains [ERROR] when an unexpected error occurred

— A job is finished with success if Job Status attribute is COMPLETED and all related Workflow Status are SUCCESS.

— A job is finished with error if Job Status attribute is COMPLETED and not all related Workflow Status are SUCCESS.

In any step, the user can read the node certificate status using the following ENM CLI command:

```
»secadm certificate get --certtype OAM --nodelist <nodelist>
```

6.3 Troubleshooting on Distribute Node Trusted Certificates

This section provides the troubleshooting steps recommended to diagnose and fix common problems while distributing node trusted certificates using the `secadm trust distribute` ENM CLI command.

Further information can be retrieved by ENM CLI online help available running the following ENM CLI command `secadm help`

If root cause is not identified, collect logs of the `secserv`, `sps`, `pkiraserv`, `mscm` (if CPP nodes involved), and `mscmce` (if `COM/ECIM` nodes involved) VMs. See the section *If Issue Suspected on Node Security* of ENM Data Collection Guidelines for further information on how to connect to the required `secserv`, `sps`, `pkiraserv`, `mscm` (if required), and `mscmce` (if required) VM.

Prerequisites

Steps

1. If the job finishes with an error, for each Workflow Status that does not have `SUCCESS` status:

    a. If Workflow Details signals a `[TIMEOUT]` condition:

    Example

    For `CPP` node types (`ERBS`, `RNC`, `RBS`, `MGW`)

    make sure that the node credentials have been created for the node using the following ENM CLI commands:

```
secadm credentials get --nodelist <node-name>
```

or

```
»cmedit get <node-name> NetworkElementSecurity.*
```

If node credentials have not been yet created, create them.

Verify that alarm supervision is enabled for that node: if it is disabled, check if, despite the workflow failure, the new trusted certificates were anyway installed onto the node by reading the node trusted certificates status.

Example

For `COM/ECIM` nodes:

Make sure that the error was not caused by a misalignment between node MOs and correspondent DPS MOs: force a resync operation on node. When the node is synchronized again, read the node trusted certificates status to verify that despite the workflow failure, the new trusted certificates are installed onto the node.

Note: If the Trust distribute command is triggered with `extca` option and the workflow failed with `TIMEOUT` error, contact External CA to find more information on failure.

b. If Workflow Details signals an `[ERROR]` condition:

Verify how many trusted certificates are already present on node. Some node types have a maximum number for trusted certificates that can be installed on node. In this case, it can be necessary to remove outdated certificates using the `secadm trust remove` command.

c. If Workflow Details signals a `[FAILURE]` condition:

Read the node trusted certificates status, the Install Error Message may provide some useful information about the root cause of failure detected on node side.

If no useful information is available, the analysis must focus on the node side as it is the node that is explicitly signaling a failure detected on its side.

2. If the job finished with success status but verifying the node trusted certificates status, it shows that the old certificates are read (old values in Serial Number):

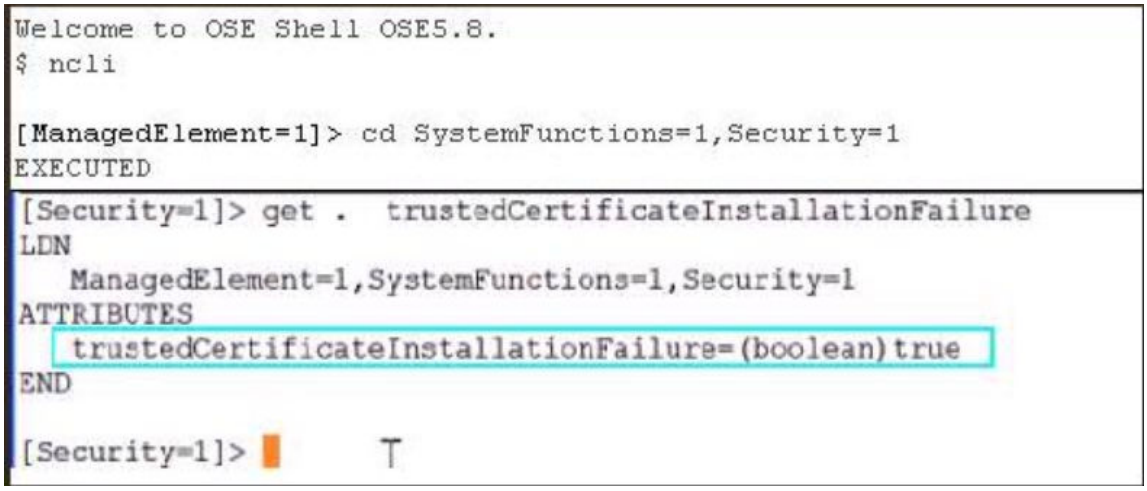
This can be caused by a misalignment between node MOs and correspondent `DPS` MOs. Force a `resync` operation on node and read the node trusted certificates status to verify that the new certificates are read (new values in Serial Number):

```
»cmedit action NetworkElement=<node-name>,CmFunction=1 sync --force
```

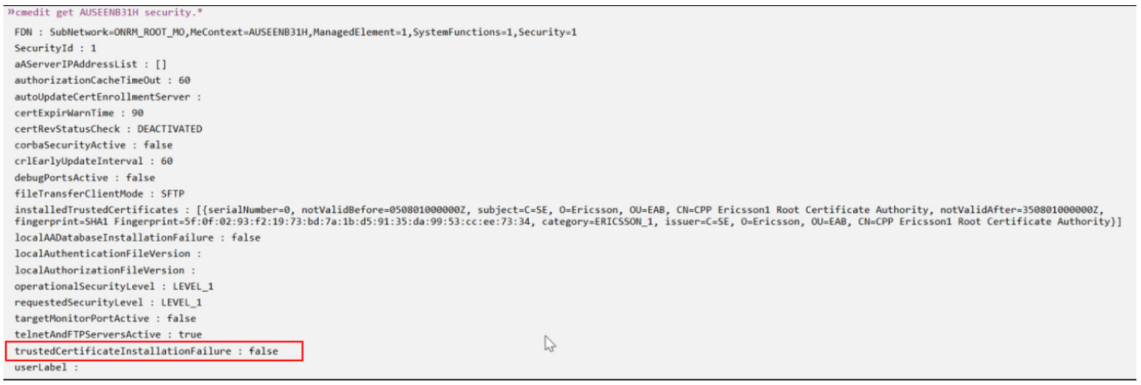
3. If the trust distribution job finishes with [TIMEOUT] status, this can be caused by a misalignment between the node MOs and corresponding ENM (DPS) MOs.

   To verify the misalignment between node and ENM (DPS), find the following information provided. The data in the figures are just for example.

   a. Verify the `trustedCertificateInstallationFailure` attribute value present on node. Connect to the node and do the steps described in the following figure to verify the attribute value present on the node:



   b. Verify the `trustedCertificateInstallationFailure` attribute value present on ENM (DPS):



   c. If there is a misalignment between `trustedCertificateInstallationFailure` attribute value on node and ENM (DPS), then trigger force sync on the node:

```
cmedit action NetworkElement=<node-name>,CmFunction=1 sync --force
```

Re-trigger the trust distribution use-case.

Results

The distribute node trusted certificates command is asynchronously managed:

A job is created (uniquely identified by a *<job-id>*) and a set of associated workflows is scheduled (one workflow for each valid node).

A response, containing the *<job-id>* and the list of specific errors for invalid nodes, is returned to the user.

Asynchronously, each workflow is executed performing the requested operations on node:

for CPP node types (ERBS, RNC, RBS, MGW), the workflow generally performs actions on node and the action progress result is available to workflow through events sent by node itself,

for COM/ECIM node types, the workflow performs actions on node and the action progress result is available by an active poll performed by workflow itself reading specific node objects.

The user can monitor the progress of the job (and of related workflows) using the following ENM CLI command:

```
secadm job get -j <job-id>
```

The response contains an overall Job Status and a Workflow Status for each workflow.

The job finishes when Job Status is set to COMPLETED.

The final status of each workflow is then available in Workflow Status:

— if it is set to SUCCESS the requested operations on that node were successful

— if it is set to ERROR the requested operations on that node failed: the user can retrieve more information on the failure from the Workflow Details:

— it contains [TIMEOUT] when an action performed on the node did not complete within maximum expected time

— it contains [FAILURE] when the node itself explicitly signaled a failure in the execution of an action

— it contains [ERROR] when an unexpected error occurred

— A job is finished with success if Job Status attribute is COMPLETED and all related Workflow Status are SUCCESS.

— A job is finished with error if Job Status attribute is `COMPLETED` and not all related Workflow Status are `SUCCESS`.

The user can, in any step, read the node trusted certificates status using the following ENM CLI command:

```
secadm trust get --certtype OAM --nodelist <nodelist>
```

6.4 Troubleshooting on Create and Update Ssh Key

This section provides the troubleshooting steps recommended to diagnose and fix common problems while creating or updating SSH key using the `secadm sshkey` ENM CLI commands.

Further information can be retrieved by ENM CLI online help:

```
»secadm help
```

If root cause is not identified, collect logs of the `secserv`, `mscm` (if CPP nodes involved), and `mscmce` (if COM/ECIM nodes involved) VMs. See the *If Issue Suspected on Node Security* section of ENM Data Collection Guide, for further information on how to connect to the required `secserv`, `mscm` (if required), and `mscmce` (if required) VM.

Steps

If command ends with success but the ENM SSH keys return that the values are `Invalid_key`:

1. Verify that the node credentials have been created for the node.

   Run the following ENM CLI command:

   ```
   »secadm credentials get --nodelist <node-name>
   ```

   or

   ```
   »cmedit get <node-name> NetworkElementSecurity.*
   ```

   If not yet created, create credentials for the node and rerun the `secadm sshkey` ENM CLI command.

6.5 Troubleshooting on Remove Node Trust Certificates

This section provides the troubleshooting steps recommended to diagnose and fix common problems while removing node trusted certificates using the `secadm trust remove` ENM CLI command.

Further information can be retrieved by ENM CLI online help:

```
»secadm help
```

If root cause is not identified, collect logs of the `secserv`, `sps`, `mscm` (if CPP nodes involved), and `mscmce` (if COM/ECIM nodes involved) VMs. See the *If Issue Suspected on Node Security* section of ENM Data Collection Guide, for further information on how to connect to the required `secserv`, `sps`, `mscm` (if required), and `mscmce` (if required) VM.

Steps

If the job finishes with an error, for each Workflow Status that does not have SUCCESS status:

1. If Workflow Details signals a [TIMEOUT] condition:

   Example

   For CPP node types (ERBS, RNC, RBS, MGW)

   Verify that alarm supervision is enabled for that node. If it is disabled, check if, despite the workflow failure, the specified trusted certificates were removed from the node by reading the node trusted certificates status.

   Example

   For COM/ECIM nodes:

   Verify that the error was not caused by a misalignment between node MOs and correspondent DPS MOs. Force a resync operation on node and, when the node is synchronized again, read the node trusted certificates status to check that despite the workflow failure, the specified trusted certificates were removed from the node.

2. If Workflow Details signals an [ERROR] condition:

   Example

   Verify if the issuer DN of the trusted certificate to be removed has the format "CN=<common name>,O=<organization>,OU=<organization unit>,C=<country>" (the fields order is not fundamental).

   If formats differ, do the following:

   For CPP node types remove the trusted certificate from ENM CLI:

   Find the FDN of involved Security MO <Security FDN>:

   ```
   »cmedit get <node-name> Security
   ```

   Perform remove action on involved Security MO specifying the wanted serial number and issuer DN:

```
»cmedit action <Security FDN> removeTrustedCert.(serialNumber=<serial number
>,issuer=<issuer DN>,category=CORBA_PEERS)
```

Check if remove has been successfully performed reading the node trusted certificates status:

```
secadm trust get --certtype OAM --nodelist <nodelist>
```

Example

For COM/ECIM nodes

Find the FDN of the TrustedCertificate MO to be removed (it has wanted certificateContent.issuer and certificateContent.serialNumber) <TrustedCertificate FDN>:

```
»cmedit get <node-name> TrustedCertificate.*
```

Find the FDN of involved CertM MO <CertM FDN>:

```
»cmedit get <node-name> CertM
```

Perform remove action on involved CertM MO specifying the wanted TrustedCertificate MO:

```
»cmedit action <CertM FDN> removeTrustedCert.(trustedCert="<TrustedCertifica
te FDN>")
```

Check if remove has been successfully performed reading the node trusted certificates status:

```
secadm trust get --certtype OAM --nodelist <nodelist>
```

3. Verify if attempting to remove the last trusted certificate for the node, for COM/ECIM nodes.

   Such operation is not allowed for ECIM nodes.

Results

The remove node trusted certificates command is asynchronously managed.

A job is created (uniquely identified by a *<job-id>*) and a set of associated workflows is scheduled (one workflow for each valid node).

A response, containing the *<>* and the list of specific errors for invalid nodes, is returned to the user. <job-id>.

Asynchronously, each workflow is executed to perform the requested operations on node:

For CPP node types (ERBS, RNC, RBS, MGW), the workflow generally performs actions on node and the action progress result is available to workflow by events sent by node itself.

For COM/ECIM node types, the workflow performs actions on node and the action progress result is available through an active poll performed by workflow itself reading specific node objects.

The user can monitor the progress of the job (and of related workflows) using the following ENM CLI command:

```
»secadm job get -j <job-id>
```

The response contains an overall Job Status and a Workflow Status for each workflow.

The job finishes when Job Status is set to COMPLETED.

The final status of each workflow is then available in Workflow Status:

— if it is set to SUCCESS, the requested operations on that node were successful.

— if it is set to ERROR, the requested operations on that node failed: the user can retrieve more information on the failure from the Workflow Details.

— it contains [TIMEOUT] when an action performed on the node did not complete within maximum expected time.

— it contains [FAILURE] when the node itself explicitly signaled a failure in the execution of an action.

— it contains [ERROR] when an unexpected error occurred.

— A job is finished with success if Job Status attribute is COMPLETED and all related Workflow Status are SUCCESS.

— A job is finished with error if Job Status attribute is COMPLETED and not all related Workflow Status are SUCCESS.

In any step, the user can read the node trusted certificates status using the following ENM CLI command:

```
»secadm trust get --certtype OAM --nodelist <nodelist>
```

6.6 Troubleshooting on Security Level Functionality

The `secadm sl set` command on WEB CLI has been executed with success but if switching to SL2 or SL1 is successful or not.

Prerequisites

— Nodes must exist in the system.

— Nodes must be synchronized.

— Enable the SHA1 algorithm to avoid the Cert Enrollment failure.

  — use the following command to check the algorithm status:

```
”pkiadm cfg algo --list --type all --status all”
```

  — use the following command to enable the SHA1 algorithm:

```
"pkiadm configmgmt algo --enable --name SHA1"
```

— Create node credentials: To create node credentials, see the *Create Node Credentials* in ENM Network Security Configuration System Administrator Guide, Reference [21].

— User needs to be a Node Security administrator to trigger the security level set command.

— FM alarmSupervisionState must be active.

  — Use the following command to activate the alarmSupervisionState on the node:

```
”alarm enable node_name"
```

  — Use the following command to check the alarmSupervisionState on the node:

```
”alarm status node_name”
```

6.6.1 Switching to Security Level 2 Success Case

For verifying whether any task is successful or not, we can get the workflow ID using the following steps.

— Search with the keyword 'CPPActivateSL2' in Logviewer.

```
INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (EJB default - 74) [administrato →
r, WorkFlow Handler [CPPActivateSL2], STARTED, Node Security Service, node [ →
NetworkElement=LTE04ERBS00001], workflow id [d56bf8db-7e38-11e6-a9c3-5254001 →
80465] : Workflow successfully started: business key [secwf_MeContext=LTE04E →
RBS00001]: params [{TRUSTED_CATEGORY=CORBA_PEERS, NODE_FDN=NetworkElement=LT →
E04ERBS00001}]].
```

— Identify the workflow ID 'd56bf8db-7e38-11e6-a9c3-525400180465' from the previously mentioned log, search with the workflow id and the message 'FINISHED_WITH_SUCCESS' appears as follows for the following tasks.

Steps

1. Verify whether the CPPInstallTrustedCertificates has FINISHED_WITH_SUCCESS and the following message appears in Logviewer:

   Result:

2. Verify whether the InitCertEnrollmentTask has FINISHED_WITH_SUCCESS and the following message appears in Logviewer:

   Result:

```
INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (EJB async - 18) [NO USER DATA, →
WorkFlow Task Handler [InitCertEnrollmentTask], FINISHED_WITH_SUCCESS, Node →
Security Service, node [LTE04ERBS00001], workflow name [CPPInitCertEnrollmen →
t] : workflow id [eb54cb87-7e38-11e6-a9c3-525400180465] : processTask InitCe →
rtEnrollmentTask for node [NodeRef{fdn='NetworkElement=LTE04ERBS00001'}] is →
finished]INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-executor-tp-thread →
s - 4) [administrator, WorkFlow Task Handler [ReadTrustedCertificateInstalla →
tionFailureTask], FINISHED_WITH_SUCCESS, Node Security Service, node [LTE04E →
RBS00001], workflow name [CPPInstallTrustedCertificates] : workflow id [d5b7 →
a7e4-7e38-11e6-a9c3-525400180465] : Return trustedCertificateInstallationFai →
lure: false]
```

3. Verify whether the EnableCorbaSecurityTask has FINISHED_WITH_SUCCESS and the following message appears in Logviewer:

   Result:

```
INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-executor-tp-threads - 7) [a →
dministrator, WorkFlow Task Handler [EnableCorbaSecurityTask], FINISHED_WITH →
_SUCCESS, Node Security Service, node [LTE04ERBS00001], workflow name [CPPAc →
tivateCorbaSecurity] : workflow id [f52304dd-7e38-11e6-a9c3-525400180465] : →
Command [SSHCommandJob [commandToExecute=secmode -l 2, toString()=MediationT →
askRequest [nodeAddress=NetworkElement=LTE04ERBS00001,SecurityFunction=1,Net →
workElementSecurity=1, jobId=LTE04ERBS00001-44d6b5fc-7b5e-4818-a062-5c5373bc →
27d9, protocolInfo=CM, clientType=null]]] sent to the node [NetworkElement=L →
TE04ERBS00001] with Success]
```

4. Verify whether the CPPActivateSL2 workflow has FINISHED_WITH_SUCCESS and the following message appears in Logviewer:

   Result:

```
INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-executor-tp-threads - 8) [a →
dministrator, WorkFlow Handler [CPPActivateSL2],
FINISHED_WITH_SUCCESS, Node Security Service, node [NetworkElement=LTE04ERBS →
```

```
00001], workflow id [d56bf8db-7e38-11e6-a9c3-525400180465] :
Workflow successfully completed.]
```

6.6.2 Switching to Security Level 2 Error Case

Perform steps 1 and 2 from Switching to Security Level 2 Success Case on page 47 to get workflow ID and if the keyword 'FINISHED_WITH_ERROR' is found at any of the following three tasks, switching to SL2 is failed.

The three tasks are ReadTrustedCertificateInstallationFailureTask, InitCertEnrollmentTask, and EnableCorbaSecurityTask.

Steps

1. Verify whether the `ReadTrustedCertificateInstallationFailureTask` has FINISHED_WITH_ERROR and the following message appears in Logviewer:

```
INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-executor-tp-threads - 4) [a
dministrator, WorkFlow Task Handler [ReadTrustedCertificateInstallationFailu
reTask],FINISHED_WITH_ERROR, Node Security Service, node [LTE04ERBS00002], w
orkflow name [CPPInstallTrustedCertificates] : workflow id [89fr7e4-7e38-11e
6-a9c3-525400180465]
```

2. Verify whether the `InitCertEnrollmentTask` has FINISHED_WITH_ERROR and the following message appears in Logviewer:

```
INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-executor-tp-threads - 19) [
administrator, WorkFlow Handler [CPPActivateSL2], FINISHED_WITH_ERROR, Node
Security Service, node [NetworkElement=LTE04ERBS00002], workflow id [ed1c75b
c-7e69-11e6-a9c3-525400180465] : Workflow failed at step [Initialize certifi
cate enrollment].]
```

3. Verify whether the `EnableCorbaSecurityTask` has FINISHED_WITH_ERROR and the following message appears in Logviewer:

```
INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-executor-tp-threads - 7) [a
dministrator, WorkFlow Task Handler [EnableCorbaSecurityTask],FINISHED_WITH_
ERROR, Node Security Service, node [LTE04ERBS00001], workflow name [CPPActiv
ateCorbaSecurity] : workflow id [5f4304dd-7e38-11e6-a9c3-525400180465] :
```

4. Verify whether SshException or the EOF error message appears in Logviewer.

```
com.ericsson.oss.mediation.transport.api.exception.TransportException:

Caused by:

com.ericsson.oss.mediation.transport.ssh.maverick.provider.exception.OpenCon
nectionException:

Caused by: com.maverick.ssh.SshException: EOF

received from remote side [Unknown cause] at
```

```
com.maverick.ssh2.TransportProtocol.readWithTimeout(TransportProtocol.java:6 →
92
```

or

```
com.ericsson.oss.mediation.transport.api.exception.TransportException:

Caused by:

com.ericsson.oss.mediation.transport.ssh.maverick.provider.exception.OpenCon →
nectionException:

SSH connection failed

Caused by: com.maverick.ssh.SshException: EOF

received from remote side [Unknown cause]
```

This issue can be related to node. Collect the Security-related node logs for CPP nodes described in the section *If Issue Suspected on Node Security* in ENM Data Collection Guideline, Reference [9], and all service group logs mentioned in the section Other Issues on page 51.

6.6.3 Switching to Security Level 1 Success Case

— Search for keyword 'CPPDeactivateSL2' in logviewer.

```
INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (EJB default - 105) [administrat →
or, WorkFlow Handler [CPPDeactivateSL2], STARTED, Node Security Service, nod →
e [NetworkElement=LTE04ERBS00001], workflow id [303fbbf7-7e52-11e6-a9c3-5254 →
00180465] : Workflow successfully started: business key [secwf_MeContext=LTE →
04ERBS00001]: params [{TRUSTED_CATEGORY=CORBA_PEERS, NODE_FDN=NetworkElement →
=LTE04ERBS00001}]]
```

— Identify the workflow ID '303fbbf7-7e52-11e6-a9c3-525400180465' from the previously mentioned log, search with the workflow ID and the message "FINISHED_WITH_SUCCESS" appears as follows:

Steps

Verify whether the `DisableCorbaSecurityTask` has FINISHED_WITH_SUCCESS and the following message appears in Logviewer.

```
INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-executor-tp-threads - 31) [admi →
nistrator, WorkFlow Handler [CPPDeactivateSL2], FINISHED_WITH_SUCCESS, Node Secu →
rity Service, node [NetworkElement=LTE04ERBS00001], workflow id 303fbbf7-7e52-11 →
e6-a9c3-525400180465] : Workflow successfully completed.]
```

6.6.4 Switching to Security Level 1 Error Case

Perform steps 1 and 2 from Switching to Security Level 1 Success Case on page 50 for success case and if the keyword "FINISHED_WITH_ERROR" is found at DisableCorbaSecurityTask, switching to SL1 is failed.

Steps

1. Verify whether the `DisableCorbaSecurityTask` has FINISHED_WITH_ERROR and the following message appears in Logviewer.

```
INFO  [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-executor-tp-threads - 9) [
administrator, WorkFlow Task Handler [DisableCorbaSecurityTask], FINISHED_WI
TH_ERROR, Node Security Service, node [LTE04ERBS00001], workflow name [CPPDe
activateCorbaSecurity] : workflow id [3056ed80-7e52-11e6-a9c3-525400180465]
:
```

2. Verify the SshException or EOF error message appears in Logviewer.

```
com.ericsson.oss.mediation.transport.api.exception.TransportException:

Caused by:

com.ericsson.oss.mediation.transport.ssh.maverick.provider.exception.OpenCon
nectionException:

Caused by: com.maverick.ssh.SshException: EOF

received from remote side [Unknown cause] at

com.maverick.ssh2.TransportProtocol.readWithTimeout(TransportProtocol.java:6
92
```

or

```
com.ericsson.oss.mediation.transport.api.exception.TransportException:
Caused by:

com.ericsson.oss.mediation.transport.ssh.maverick.provider.exception.OpenCon
nectionException:

SSH connection failed

Caused by: com.maverick.ssh.SshException: EOF

received from remote side [Unknown cause]
```

This issue can be related to node. Collect the Security-related node logs for CPP nodes described in the section *If Issue Suspected on Node Security* in ENM Data Collection Guidelines,[9], and all service group logs mentioned in the section Other Issues on page 51.

6.6.5 Other Issues

If any other issue is found, collect logs of the following Service Groups:

- `secserv`
- `sps`
- `pkiraserv`
- `mscm`

— mscmce

6.7 Troubleshooting on Download CRL on Demand

The `secadm crl download` command on ENM CLI has been executed with success message but CRLs are not downloaded on the nodes.

Prerequisites

— CDPS extension must be present in all the certificates of CA and End Entity.

— Node must have CRL Check attribute activated at least once and TLS/IPSec connection to ENM service must be re-established at least once after activating the CRL Check.

6.7.1 COM/ECIM Nodes

1. Execute the following command on ENM CLI to verify CRL download on COM/ECIM Node.

```
cmedit get ManagedElement=LTE01dg2ERBS00001,SystemFunctions=1,SecM=1,CertM=1
```

The sample output is as follows:

```
»cmedit get ManagedElement=LTE01dg2ERBS00003,SystemFunctions=1,SecM=1,CertM=1
FDN : ManagedElement=LTE01dg2ERBS00003,SystemFunctions=1,SecM=1,CertM=1
localFileStorePath : null
certMId : 1
userLabel : null
reportProgress : {timeOfLastStatusUpdate=2016-12-13T12:16:52, result=SUCCESS, progressInfo=, state=FINISHED,
actionName=downloadCrl, timeActionStarted=2016-12-13T12:16:52, progressPercentage=100, actionId=6,
timeActionCompleted=2016-12-13T12:16:52, resultInfo=No CRLs stored in node}
```

2. If reportProgress contains actionName as downloadCrl and resultInfo contains No CRLs stored in node, then no CRL is downloaded on the node. This is considered as failure. Check whether the prerequisites are met or not.
3. If any other issue is found, collect logs of the following Service Groups:

— secserv

— pkiraserv

— mscm

— mscmce

6.7.2 CPP Nodes

1. Log on the node with Shell Terminal in **ENM Launcher** page to check CRL download on the node.
2. Run `crlinfo` command to check the CRLs information on the node. Check for the latest CRL on the node.

   ```
   RBS548> crlinfo
   ```

3. Check for the latest CRL in the previous command output.

   If it does not exist, check the logviewer in ENM to know whether download CRL request reached ENM.

4. Search with the keyword 'PKI_CDPS.CRL_DOWNLOAD && ENM_OAM_CA' in logviewer to check the download of ENM_OAM_CA crl.

   ```
   INFO [com.ericsson.oss.itpf.EVENT_LOGGER] (http-executor-threads - 4) [NO US →
   ER DATA, PKI_CDPS.CRL_DOWNLOAD, COARSE, CDPSService, CRLClient, Requested CR →
   L file is downloaded from CDPS Service for the CAName ENM_OAM_CA and Certifi →
   cate Serial Number :6c79de8932ceaa37]
   ```

5. Collect logs of the following Service Groups to check the issue, if this information has not been found on ENM.

   — `secserv`

   — `pkiraserv`

   — `mscm`

   — `mscmce`

6.8 Troubleshoot Enable, Disable, and Read CRL Check

Use this procedure to troubleshoot issues that occur while enabling, disabling, or reading CRL Check.

Prerequisites

— Nodes exist in the system.

— Nodes are synchronized.

— Online IPSec/OAM Certificate Enrollment is completed on the Nodes.

Steps

1. Perform the procedure described in *CRL check enable or disable webcli command limitation for Baseband Radio and Baseband Radio T node of Limitations* section of the ENM Network Security Configuration System Administrator Guide [21] to verify and to enable or disable CRL Check using `cmedit set` command.

   Even if all the prerequisites are met, enabling or disabling CRL Check is failed with the error message `Trust Category MO does not exist for the given node` and error code `10101` for Baseband Radio and Baseband Radio T node, then the cause for the failure can be more than one `Ikev2PolicyProfile MO` present on the node.

2. Collect logs of the following Service Groups for further analysis, if any other issue is found.

   — `secserv`

   — `mscm`

   — `mscmce`

6.9 CRL Check on Node Is Not Working after Enabling CRL Feature

This task describes how to troubleshoot if Certificate Revocation check functionality does not work on the node even after enabling CRL check feature.

Prerequisites

— CRL check is enabled on the node.

  Refer to *Read Certificate Revocation Check Status on Nodes* section of the ENM Public Key Infrastructure System Administrator Guide.

— CDPS extension is present in all End Entity and CA Certificates.

Steps

1. Check if all the preconditions have been met.

2. After Certificate Revocation Check is enabled on the G1/G2 (CPP, COM/ECIM) nodes, revoke the Peer Certificate and execute the following steps.

   Therefore, the node verifies the Peers Certificate revocation status from the next communication and rejects it. The user with `Cmedit_Administrator` role can execute the following commands:

```
cmedit set NetworkElement=<Node_Name>,CmNodeHeartbeatSupervision=1 active=fa →
lse
cmedit action NetworkElement=<Node_Name>,CmFunction=1 sync
cmedit set NetworkElement=<Node_Name>,CmNodeHeartbeatSupervision=1 active=tr →
ue
cmedit action NetworkElement=<Node_Name>,CmFunction=1 sync
```

3. If the issue persists, there can be multiple reasons for the failure:
   - `MSCM` service certificate is revoked but CRL is not generated for that issuer.
   - `MSCM` service certificate is revoked and CRL is generated for that, but not published to CDPS.
   - CRL is published to CDPS, but node did not download the latest CRL.

Results

If the CRL feature is working, the node does not establish any communication with ENM services.

6.10 Troubleshooting on Set and Get Ciphers on Nodes

This task describes how to troubleshoot issues that occur during set and get ciphers on nodes.

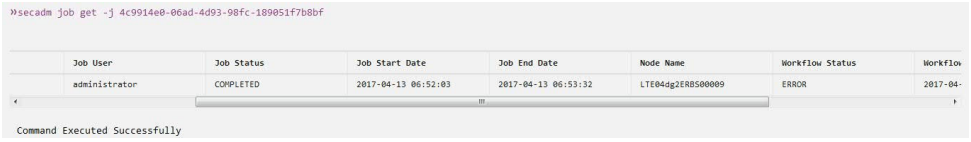
Prerequisites

- Nodes must exist in the system.
- Nodes must be synchronized.
- OAM Certificate enrollment must be done on Nodes for setting ciphers for TLS protocol.
- `cipherfilter` property value must have valid cipher strings for setting ciphers for TLS protocol.

Steps

1. Verify whether all the preconditions have been met if the command response contains error message.
2. Collect logs of the following Service Groups if the command is executed successfully and 'Workflow status' is 'ERROR' in the job id as shown in the following figure or any other issue is found.
   - `secserv`
   - `mscm`

— mscmce



6.11 Enrollment/SL2 Error 'Automatic PKI Credentials Management Job Failed due to: Null'

This section describes the work-around for Enrollment/SL2 use-cases, which fail with the error `Automatic PKI credentials management job failed due to: null`.

Prerequisites

— Access to Master Server.

Problem Description

The Enrollment/SL2 use-cases fail with the error `Automatic PKI credentials management job failed due to: null`.

One of the `sps` entities (for example, svc-4-sps_INFRASTRUCTURE_PKI_MANAGER) is not created in the PKI core database even though it is created in the manager database.

— pkimanager DB

```
pkimanagerdb=# select name from entity where name like '%INFRASTRUCTURE_PKI_MANAGER';
                name
-------------------------------------
 svc-4-sps_INFRASTRUCTURE_PKI_MANAGER
 svc-2-sps_INFRASTRUCTURE_PKI_MANAGER
 svc-1-sps_INFRASTRUCTURE_PKI_MANAGER
 svc-3-sps_INFRASTRUCTURE_PKI_MANAGER
(4 rows)
```

— pkicore DB

```
pkicoredb=#  select name from entity_info where name like '%INFRASTRUCTURE_PKI_MANAGER';
                name
-------------------------------------
 svc-3-sps_INFRASTRUCTURE_PKI_MANAGER
 svc-2-sps_INFRASTRUCTURE_PKI_MANAGER
 svc-1-sps_INFRASTRUCTURE_PKI_MANAGER
(3 rows)
```

— Entity for svc-4-sps_INFRASTRUCTURE_PKI_MANAGER

Name	Type	Entity Status	Certificates Assigned
svc-2-sps_INFRASTRUCTURE_PKI_MANAGER	End Entity	ACTIVE	13
svc-1-sps_INFRASTRUCTURE_PKI_MANAGER	End Entity	ACTIVE	13
svc-3-sps_INFRASTRUCTURE_PKI_MANAGER	End Entity	ACTIVE	14
svc-4-sps_INFRASTRUCTURE_PKI_MANAGER	End Entity	NEW	0

Log Description

```
2017-08-04 07:48:02,671 INFO [com.ericsson.oss.itpf.security.pki.core.common.per
sistence.handler.CertificatePersistenceHelper] (EJB default - 116) CertificateDa
ta stored in PKI Core database.
2017-08-04 07:48:02,672 ERROR [org.jboss.as.ejb3] (EJB default - 116) JBAS014268
: Failure in caller transaction.: java.lang.NullPointerException
 at com.ericsson.oss.itpf.security.pki.core.common.persistence.handler.Certifica
tePersistenceHelper.makeEntityCertificateInActive(CertificatePersistenceHelper.j
ava:556) [pki-core-common-jar-1.30.1.jar:1.30.1]
```

```
2017-08-04 07:48:02,696 ERROR [com.ericsson.oss.itpf.security.pki.manager.servic
e.schedular.PkiCredentialsManagementTimerServiceBean] (EJB default - 116) Automa
tic pki credentials management job failed due to :null
2017-08-04 07:48:02,697 ERROR [com.ericsson.oss.itpf.ERROR_LOGGER] (EJB default
- 116) [OU=BUCI_DUAC_NAM,O=ERICSSON,C=SE,CN=CREDMAPIsvc-3-pkiraserv, PKI_MANAGER
_CREDENTIALS_MANAGEMENT_TIMER.CREDENTIAL_GENERATION_FAILURE, CRITICAL, PkiCreden
tialsManagementTimerServiceBean, Generation of Pki credentials, Automatic pki cr
edentials management job failed due to :null]
```

Steps

1. Connect to the `pkimanagerdb`.

   ```
   /opt/rh/postgresql92/root/usr/bin/psql -U postgres -d pkimanagerdb
   ```

2. Delete the entity that has no certificates (entity with `NEW` status, in this case entity is `svc-4-sps_INFRASTRUCTURE_PKI_MANAGER`)

   ```
   pkimanagerdb=# delete from entity where name='svc-4-sps_INFRASTRUCTURE_PKI_M
   ANAGER';
   DELETE 1
   ```

   ```
   pkimanagerdb=# delete from entity where name='svc-4-sps_INFRASTRUCTURE_PKI_MANAGER';
   DELETE 1
   pkimanagerdb=# select name from entity where name like '%INFRASTRUCTURE_PKI_MANAGER';
                     name
   -------------------------------------
    svc-2-sps_INFRASTRUCTURE_PKI_MANAGER
    svc-1-sps_INFRASTRUCTURE_PKI_MANAGER
    svc-3-sps_INFRASTRUCTURE_PKI_MANAGER
   (3 rows)
   ```

3. For failure scenario, timer runs automatically for every minute and generates the entity and its certificate in both the`pkimanagerdb` and `pkicoredb`.

```
pkimanagerdb=# select name from entity where name like '%INFRASTRUCTURE_PKI_MANAGER';
                name
-------------------------------------
 svc-2-sps_INFRASTRUCTURE_PKI_MANAGER
 svc-1-sps_INFRASTRUCTURE_PKI_MANAGER
 svc-3-sps_INFRASTRUCTURE_PKI_MANAGER
 svc-4-sps_INFRASTRUCTURE_PKI_MANAGER
(4 rows)
```

```
pkicoredb=# select name from entity_info where name like '%INFRASTRUCTURE_PKI_MANAGER';
                name
-------------------------------------
 svc-3-sps_INFRASTRUCTURE_PKI_MANAGER
 svc-2-sps_INFRASTRUCTURE_PKI_MANAGER
 svc-1-sps_INFRASTRUCTURE_PKI_MANAGER
 svc-4-sps_INFRASTRUCTURE_PKI_MANAGER
(4 rows)
```

4. Perform the enrollment/SL2 and verify that it is successful.

Results

Enrollment/SL2 is successful.

6.12 Troubleshooting IPsec CLI Management

Use this procedure to diagnose when the `secadm IPsec` command on ENM CLI has been executed with success but if `IPSec` activation or deactivation is not successful.

Prerequisites

— Nodes must be synchronized.

— Root access to the ENM.

— Enable the SHA1 algorithm to avoid Certificate Enrollment failure.

Use the following command to check the algorithm status:

```
pkiadm cfg algo --list --type all --status all
```

— If SHA1 algorithm is disabled, use the following command to enable it:

```
pkiadm configmgmt algo --enable --name SHA1
```

It is necessary to have FM supervision enabled on the node. Use the following command to check *<alarmSupervisionState>* on the node:

```
alarm status <nodename>
```

— If *<alarmSupervisionState>* is not enabled, use the following command to enable it:

```
fmedit set NetworkElement= <nodename>,FmAlarmSupervision=1 alarmSupervisionS →
tate=true
```

— The certificate-based authentication must be enabled for IPsec at Security Gateway.

— The variable *<ossCorbaNameServiceAddress>* must be set on the Node under `RbsConfiguration MO`. If it is not set, connect to the Management Server (MS) for physical deployments or connect to VNF-LAF for cloud deployments.

If the Node IP Address is of type `IPV4`, use the following command:

```
cat /etc/hosts | grep visinamingsb-pub
```

Copy the *<visinamingsb-pub>* address and set the same to *<ossCorbaNameServiceAddress>* variable by using the following `cmedit` command from ENM CLI:

```
cmedit set MeContext=<node_name>,ManagedElement=1,NodeManagementFunction=1,R →
bsConfiguration=1 ossCorbaNameServiceAddress=<visinamingsb-pub_address>
```

If the Node IP Address is of type `IPV6`, use the following command:

```
cat /ericsson/tor/data/global.properties | grep visinamingsb_service_IPv6_IP →
s
```

Copy the *<visinamingsb_service_IPv6_IPs>* address and set the same to *<ossCorbaNameServiceAddress>* variable using the following `cmedit` command from ENM CLI:

```
cmedit set MeContext=<node_name>,ManagedElement=1,NodeManagementFunction=1,R →
bsConfiguration=1 ossCorbaNameServiceAddress=<visinamingsb_service_IPv6_IPs_ →
address>
```

Steps

`Troubleshooting on Activate IPsec for OAM`

To verify if any task is successful, it is necessary to get the workflow ID. To do this, search with the keyword *<Node_Name> && CPPActivateIpSec* in Log Viewer.

```
INFO  [com.ericsson.oss.itpf.COMMAND_LOGGER] (EJB default - 52) [Administrator,
WorkFlow Handler [CPPActivateIpSec], STARTED, Node Security Service, node [Netwo
rkElement=LTE08ERBS00001], workflow id [a29237ea-f75d-11e7-b1ba-52540044447f] :
Workflow successfully started: business key [secwf_MeContext=LTE08ERBS00001]: pa
rams [{NODE_FDN=NetworkElement=LTE08ERBS00001, SUB_ALT_NAME=192.168.100.217, NOD
ES_XML=<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Nodes>
    <Node>
        <NodeFdn>LTE08ERBS00001</NodeFdn>
        <SubAltName>192.168.100.217</SubAltName>
        <SubAltNameType>IPV4</SubAltNameType>
        <EnableOMConfiguration1>
            <removeTrustOnFailure>true</removeTrustOnFailure>
            <trustedCertificateFilePath>IPSEC</trustedCertificateFilePath>
            <dnsServer1>10.0.0.1</dnsServer1>
            <dnsServer2>10.0.0.2</dnsServer2>
            <ipAddressOaMInner>192.168.100.100</ipAddressOaMInner>
            <networkPrefixLength>24</networkPrefixLength>
            <ipAccessHostEtId>2</ipAccessHostEtId>
            <defaultrouter0>10.10.10.1</defaultrouter0>
            <ipAddressOaMOuter>192.168.100.217</ipAddressOaMOuter>
            <remoteIpAddress>10.10.4.2</remoteIpAddress>
            <remoteIpAddressMask>20</remoteIpAddressMask>
            <peerOaMIpAddress>10.10.4.10</peerOaMIpAddress>
            <peerIdentityIdFqdn>SeGW1.LTERAN.example.com</peerIdentityIdFqdn>
            <peerIdentityIdType>IP_V4_ADDRESS</peerIdentityIdType>
            <tsLocalIpAddressMask>24</tsLocalIpAddressMask>
            <tsRemoteIpAddressRanges>
                <ipAddress>10.10.2.1</ipAddress>
                <mask>0</mask>
            </tsRemoteIpAddressRanges>
            <ipSecTunnelAllowedTransforms>
                <ipSecTunnelAllowedTransform>
                    <encryptionAlgorithm>AES_CBC_128</encryptionAlgorithm>
                    <integrityAlgorithm>HMAC_SHA_1_96</integrityAlgorithm>
                </ipSecTunnelAllowedTransform>
            </ipSecTunnelAllowedTransforms>
            <ikePeerAllowedTransforms>
                <ikePeerAllowedTransform>
                    <diffieHellmanGroup>GROUP_2</diffieHellmanGroup>
                    <encryptionAlgorithm>AES_CBC_128</encryptionAlgorithm>
                    <integrityAlgorithm>HMAC_SHA_1_96</integrityAlgorithm>
                    <pseudoRandomFunction>HMAC_SHA1</pseudoRandomFunction>
                </ikePeerAllowedTransform>
            </ikePeerAllowedTransforms>
            <vid>1</vid>
        </EnableOMConfiguration1>
    </Node>
</Nodes>
, SUB_ALT_NAME_TYPE=IPV4}]]
```

Identify the workflow ID *<a29237ea-f75d-11e7-b1ba-52540044447f>* for the corresponding `NetworkElement`, search with the workflow id and the message `FINISHED_WITH_SUCCESS` is displayed for the following tasks:

1. Verify that the workflow `CPPInitCertEnrollmentIpSec` has `FINISHED_WITH_SUCCESS` and the following message is displayed in Log Viewer:

```
2018-01-04 05:54:41,879 INFO  [com.ericsson.oss.itpf.COMMAND_LOGGER] (EJB de
fault - 86) [NO USER DATA, WorkFlow Task Handler [InitCertEnrollmentIpSecTas
k], FINISHED_WITH_SUCCESS, Node Security Service, node [LTE08ERBS00001], wor
kflow name [CPPInitCertEnrollmentIpSec] : workflow id [9253fd65-f113-11e7-a0
c9-52540044447f] : IPsec [LTE08ERBS00001] : Certificate enrollment on Node:
NetworkElement=LTE08ERBS00001 is finished.]
```

2. Verify that the workflow CPPInstallTrustedCertificatesIpSec has FINISHED_WITH_SUCCESS and the following message is displayed in Log Viewer:

```
2018-01-04 05:54:42,709 INFO  [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-ex →
ecutor-tp-threads - 5) [NO USER DATA, WorkFlow Task Handler [ReadTrustedCert →
ificateInstallationIpSecStateTask], FINISHED_WITH_SUCCESS, Node Security Ser →
vice, node [LTE08ERBS00001], workflow name [CPPInstallTrustedCertificatesIpS →
ec] : workflow id [c1ed339d-f113-11e7-a0c9-52540044447f] : ReadTrustedCertIn →
stallationIpSecStateTaskHandler.processTask() exiting - TRUSTED_CERT_INST_ST →
ATE for node NetworkElement=LTE08ERBS00001 is 'IDLE'.]
```

3. Verify that the workflow task ChangeIpForOMSettingTask has FINISHED_WITH_SUCCESS and the following message is displayed in Log Viewer:

```
2018-01-04 05:55:05,655 INFO  [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-ex →
ecutor-tp-threads - 6) [NO USER DATA, WorkFlow Task Handler [ChangeIpForOMSe →
ttingTask], FINISHED_WITH_SUCCESS, Node Security Service, node [LTE08ERBS000 →
01], workflow name [CPPActivateIpSecurity] : workflow id [ce3e2037-f113-11e7 →
-a0c9-52540044447f] : ChangeIpForOMSettingTask completed]
```

4. Verify that the workflow CPPActivateIpSec has FINISHED_WITH_SUCCESS and the following message is displayed in Log Viewer:

```
2018-01-04 05:55:15,963 INFO  [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-ex →
ecutor-tp-threads - 7) [NO USER DATA, WorkFlow Handler [CPPActivateIpSec], F →
INISHED_WITH_SUCCESS, Node Security Service, node [NetworkElement=LTE08ERBS0 →
0001], workflow id [91f90d1a-f113-11e7-a0c9-52540044447f] : Workflow success →
fully completed with jobID: N/A, wfStatusId: null, activationStep: CPP Clean →
up M2M User and SMRS]
2018-01-04 05:55:16,046 INFO  [com.ericsson.oss.services.nscs.workflow.NscsW →
orkflowNodeStatusDataHandlerImpl] (job-executor-tp-threads - 7) Detected com →
pleted workflow CPPActivateIpSec for node NetworkElement=LTE08ERBS00001
```

Troubleshooting on Deactivate IPsec for OAM

To verify if any task is successful, it is necessary to get workflow ID. To do this, search with the keyword *<Node_Name> && CPPDeactivateIpSec* in Log Viewer.

```
INFO  [com.ericsson.oss.itpf.COMMAND_LOGGER] (EJB default- 19) [Administrator, W →
orkFlow Handler [CPPDeactivateIpSec], STARTED, Node Security Service, node [Netw →
orkElement=LTE08ERBS00001], workflow id [60fa0faa-f114-11e7-a0c9-52540044447f] : →
 Workflow successfully started: business key [secwf_MeContext=LTE08ERBS00001]: p →
arams [{REMOVE_CERT=false, NODE_FDN=NetworkElement=LTE08ERBS00001, TRUST_SERIAL_ →
NUMBER=-1, NODES_XML=<?xml version="1.0"encoding="UTF-8"standalone="yes"?>
<Nodes>
    <Node>
        <NodeFdn>LTE08ERBS00001</NodeFdn>
        <SubAltName>192.168.100.217</SubAltName>
        <DisableOMConfiguration>
            <removeCert>false</removeCert>
            <dnsServer1>10.0.0.1</dnsServer1>
            <dnsServer2>10.0.0.2</dnsServer2>
            <ipAddressOaMOuter>192.168.100.217</ipAddressOaMOuter>
            <defaultRouter0>10.10.10.1</defaultRouter0>
            <networkPrefixLength>23</networkPrefixLength>
            <remoteIpAddress>10.10.10.5</remoteIpAddress>
            <remoteIpAddressMask>20</remoteIpAddressMask>
            <vid>1</vid>
        </DisableOMConfiguration>
    </Node>
```

```
</Nodes>
, TRUST_ISSUER=null}]]
```

Identify the workflow ID `60fa0faa-f114-11e7-a0c9-52540044447f` for the corresponding `NetworkElement`, search with the workflow ID and the message `FINISHED_WITH_SUCCESS` is displayed as follows:

```
INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-executor-tp-threads - 8) [NO US →
ER DATA, WorkFlow Handler [CPPDeactivateIpSec], FINISHED_WITH_SUCCESS, Node Secu →
rity Service, node [NetworkElement=LTE08ERBS00001], workflow id [60fa0faa-f114-1 →
1e7-a0c9-52540044447f] : Workflow successfully completed with jobID: N/A, wfStat →
usId: null, activationStep: Deactivate IpSec]
```

5. Verify that the workflow `CPPDeactivateIpSec` has `FINISHED_WITH_SUCCESS` and the following message is displayed in Log Viewer:

   ```
   INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-executor-tp-threads - 8) [N →
   O USER DATA, WorkFlow Handler [CPPDeactivateIpSec], FINISHED_WITH_SUCCESS, N →
   ode Security
   ```

Activation or Deactivation Error Case

6. If there is no `IpHostLink MO` on the node, see the following error in the node logs:

   ```
   [2017-12-04 21:10:01.756] [000100]se.ericsson.crbs.cat.mao.rbsconfiguration. →
   ipforoamsetting:RequestProcessor-4 IpOamConfigurationServiceImpl:0 ENTER:get →
   AllMosOfType(IpHostLink)
   [2017-12-04 21:10:01.757] [000100]se.ericsson.crbs.cat.mao.rbsconfiguration. →
   ipforoamsetting:RequestProcessor-4 IpOamConfigurationServiceImpl:0 RETURN:ge →
   tAllMosOfType(IpHostLink)
   [2017-12-04 21:10:01.759] [000100]se.ericsson.cello.configirpimpl:RequestPro →
   cessor-4 DynMoAccess:0 ERROR:invoke action exception:
   java.lang.IndexOutOfBoundsException
   at java.util.ArrayList.get(Unknown Source)
   at se.ericsson.crbs.cat.mao.rbsconfiguration.ipforoamsetting.IpOamConfigurat →
   ionServiceImpl.notifyOssOfChangedIpAddress(Unknown Source)
   at se.ericsson.crbs.cat.mao.rbsconfiguration.actions.ChangeIpForOamSettingAc →
   tion.configurationRollback(Unknown Source)
   [2017-12-04 21:10:01.760] [000100]se.ericsson.cello.configirpimpl:RequestPro →
   cessor-4 DynMoAccess:0 ERROR:<continued>
   at se.ericsson.crbs.cat.mao.rbsconfiguration.actions.ChangeIpForOamSettingAc →
   tion.doPreConfiguration(Unknown Source)
   at se.ericsson.crbs.cat.mao.rbsconfiguration.actions.ChangeIpForOamSettingAc →
   tion.execute(Unknown Source)
   at se.ericsson.crbs.cat.mao.rbsconfiguration.RbsConfigurationMaoImpl.actionC →
   hangeIpForOamSetting(Unknown Source)
   [2017-12-04 21:10:01.760] [000100]se.ericsson.cello.configirpimpl:RequestPro →
   cessor-4 DynMoAccess:0 ERROR:<continued>
   at java.lang.reflect.AccessibleObject.invokeV(Unknown Source)
   at java.lang.reflect.Method.invoke(Unknown Source)
   at se.ericsson.cello.configirpimpl.DynMoAccess.invokeAction(Unknown Source)
   at se.ericsson.cello.configirpimpl.BasicConfigImpl.action(Unknown Source)
   at ConfigExtended.ConfigurationExtendedPOA._invoke(Unknown Source)
   ```

   Solution: Create the `IpHostLink MO` on the node which contains the node OAM outer `ip` address. The same address should be used to sync the node in ENM. The attribute `ipInterfaceMoRefvalue` under `IpHostLink MO` contains the reference to the `IPInterface MO`.

7. If the variable *<ossCorbaNameServiceAddress>* is not set on the Node under `RbsConfiguration MO`, the following error is displayed in node logs:

```
[2017-11-30 21:43:13.964] [000100]se.ericsson.crbs.cat.mao.rbsconfiguration:
CrbsGoamLm_ConfigurationReportLoggerThread RbsConfigurationMaoImpl:0 RETURN:
setReadOnlyAttribute()
[2017-11-30 21:43:13.964] [000100]se.ericsson.crbs.cat.mao.rbsconfiguration:
CrbsGoamLm_ConfigurationReportLoggerThread RbsConfigurationMaoImpl:0 RETURN:
updateAttribute(StringBuffer)
[2017-11-30 21:43:14.798] [000100]se.ericsson.crbs.cat.mao.rbsconfiguration:
RequestProcessor-5 RbsConfigurationFailedException:0 TRACE5:
Action changeIpForOamSetting() failed.
Rollback has been performed. The node is back on the initial configuration.
Failed to notify the OSS of rollback.
Notification of new OAM IP address to OSS failed.
The NodeIpAddressChange service could not be retrieved from name service.
```

Solution: Set the variable *<ossCorbaNameServiceAddress>* as outlined in the prerequisites section.

8. When `IPSec` activation and `ip address` change in ENM is complete, if the node state in ENM is either `ATTRIBUTE` or `TOPOLOGY` for an extended period, connect to the node through MO shell and provide the command `route`.

```
CELL37> route
Please enter Node Password:

171220-16:49:43 10.163.155.10 17.0g ERBS_NODE_MODEL_H_1_227 stopfile=/tmp/20
470
$ route
NOTE! Due to high memory requirements of "route", the command has been chang
ed to "route -n".
Destination                                Gateway
       Mask                                        Flags  Metric Interface
0.0.0.0                                    10.163.156.1
       0.0.0.0                                     UGS        64 le0   #2
0.0.0.0                                    10.163.155.10
       0.0.0.0                                     UGS       500 lh0   #3
10.163.156.0                               link#2
       255.255.255.0                               UC           0 le0   #2
10.163.156.1                               00:00:0c:9f:f2:c2
                                                   UHLP         0 le0   #2
10.163.156.2                               64:f6:9d:cf:c5:3c
                                                   UHLP         0 le0   #2
10.163.156.37                              74:c9:9a:43:1d:d4
                                                   UHLP         0 lo0   #1
127.0.0.1                                  127.0.0.1
                                                   UH           0 lo0   #1
169.254.1.1                                10.163.155.10
                                                   UH           0 lh0   #3
::1                                        link#1
                                                   UHL          0 lo0   #1
ff01:1::                                   ::1
       ffff:ffff::                                 UC           0 lo0   #1
ff02:1::                                   ::1
       ffff:ffff::                                 UC           0 lo0   #1
$
```

In the event that `lh0` is being used as the interface, `lh0` Metric should be smaller that `le0` metric. This can be updated by using the following sample command. Change the `ip` address accordingly.

```
CELL37> route change -net 0.0.0.0 -netmask 0.0.0.0 10.163.155.10 -hopcount 5
0
```

When command is completed, change `CmNodeHeartbeatSupervision` to `false` and then `true`.

a. Change `CmNodeHeartbeatSupervision` to `false`

```
cmedit set NetworkElement=<node_name>,CmNodeHeartbeatSupervision=1 →
active=false
```

b. Change `CmNodeHeartbeatSupervision` to `true`

```
cmedit set NetworkElement=<node_name>,CmNodeHeartbeatSupervision=1 →
active=true
```

c. Perform the action `sync`:

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

9. As part of the `ipsec` deactivation scenario, all the MOs (`IPSecTunnel`,`IkePeer`,`VpnInterface` and `IpAccessHostEt`) are deleted and the `ipInterfaceMoRef` attribute under `IpHostLink MO` is pointed to `IpInterface MO`. Hence, the MOs which belong to `IPSec` for OAM are not be referred by `IPSec` Traffic. If `IPSec` Traffic refers to the same MOs, deactivation fails and the MOs are not deleted

6.13 Troubleshooting LAAD Files Distribution

> This procedure describes how to troubleshoot issues that occur during Local Authentication and Authorization Database (LAAD) files distribution to nodes.

Prerequisites

— Nodes must be synchronized.

— Secure User credentials must be created on node.

— FM Alarm Supervision State must be enabled.

Steps

1. Distribute LAAD Files to node(s) Error Case: User with Security Management Profile not Found.

   Execute the steps described in the section Distribute LAAD Files to Nodes Error Case: User with Security Management Profile not Found on page 65.

2. Execute Other Issues.

   If any other issue is found, collect logs of the following Service Groups:

   - `secserv`
   - `mscm`
   - `sps`
   - `accesscontrol`
   - `openidm`
   - `httpd`
   - `smrserv`
   - `node logs`

   See the document ENM Data Collection Guidelines, [9], for more details about how to collect respective service group and node logs.

6.13.1 Distribute LAAD Files to Nodes Error Case: User with Security Management Profile not Found

If at least one user is not assigned with SecurityManagement task profile, then the following error message is displayed in Logviewer.

Steps

1. Verify that job finishes with `Workflow Status` as `ERROR` and `Workflow Details` signals a `[TIMEOUT]` condition:

2. Verify whether `user with Security Management Profile not found` error message appears in Logviewer.

```
2018-10-23 10:29:05,444 ERROR [com.ericsson.oss.services.security.accesscont →
rol.cppaa.laad.impl.LaadServiceImpl] (job-executor-tp-threads - 5) Error occ →
ured while retrieving the data from IDM service: [user with Security Managem →
ent Profile not found]
2018-10-23 10:29:05,444 INFO  [com.ericsson.oss.itpf.SECURITY_EVENT_LOGGER]  →
(job-executor-tp-threads - 5) [NO USER DATA, CPP AA Service, LaadServiceImpl →
, Error occured while retrieving the data from IDM service: [{}] , fetching  →
laad data from IDM, ERROR, FAILURE]
```

3. Verify whether the `CppGetLaadFilesTask has FINISHED_WITH_ERROR` message appears in Logviewer.

```
2018-10-23 10:29:05,485 INFO  [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-ex →
ecutor-tp-threads - 5) [NO USER DATA, WorkFlow Task Handler [CppGetLaadFiles →
Task], FINISHED_WITH_ERROR, Node Security Service, node [LTE02ERBS00001], wo →
rkflow name [CPPLaadFilesCreationAndDistribution] : workflow id [122c5336-d6 →
a6-11e8-af0f-525400190d0f] : Exception: com.ericsson.oss.services.security.a →
ccesscontrol.cppaa.laad.api.exception.LaadDataRetrievalException Msg: Error  →
occured while retrieving the data from IDM service: [{}]  Performing: Get an →
d Uploading LAAD Files to SMRS LAAD Files Upload Status: FAILURE for Node LT →
E02ERBS00001]
```

Troubleshooting:
Solution for the error:

At least one user must have assigned with SecurityManagement Task Profile as follows.

The procedure for creation of users and association of task profiles can be done through RESTful User Management and UI Management.

— See the document ENM Identity and Access Management Programmers Guide, 19817-cna 403 3016 [24], for interacting with the RESTful user management.

— See the document ENM Identity and Access Management System Administrator Guide, 2/1543-AOM 901 151-1 [20], for more details on users and their access control management through the concept of roles and target groups.

Creating users and association of task profiles to the user can be done through **Launcher** UI. See `online help` for more details.

6.14 Troubleshooting Trusted NTP Server

> This procedure describes how to troubleshoot the issues that occur during configure, remove, and list NTP operations on the node.

Prerequisites

— Trusted NTP server must be configured and enabled. For detailed information on the Trusted NTP server configuration, see the section *Trusted NTP Server Configuration in ENM* in the document ENM Operators Guide, Reference [3].

— User needs NodeSecurity_Administrator role to perform Configure and Remove operations and both NodeSecurity_Administrator role and NodeSecurity_Operator role to perform List operation.

— Node must be in sync with ENM.

— The following CPP and Baseband Radio Nodes are supported as part of this feature.

Table 2

neType	Version
eNodeB	>= 19.Q3
RBS	>= 19.Q3
RNC	>= 19.Q3
MGW	>= 6.10.4.0
RadioNode	>= 19.Q3

— For supported CPP nodes, the following fields must be present under "TimeSetting" MO:

  — installedNtpKeyIds attribute

  — installNtpKeys and removeNtpKeys action which has value as "Yes".

— For supported Baseband nodes, supportedAlgorithm attribute must be present under `Ntpserver` MO.

Steps

NTP Configure: the following ERRORS appears when the preconditions have not been met.

1. Verify that node has supported MOs for G2 nodes.

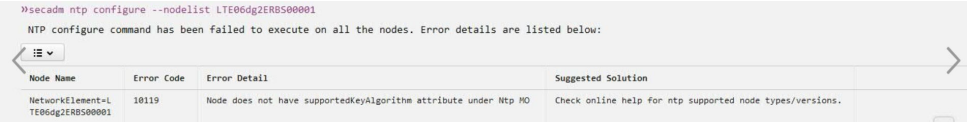


Figure 7

```
2019-12-05 11:40:26,177 ERROR [com.ericsson.nms.security.nscs.data.moget.imp →
l.ComEcimMOGetServiceImpl] (EJB default - 86)
Node [MeContext=LTE06dg2ERBS00001] doesn't have supportedKeyAlgorithm attrib →
ute under Ntp MO.
```

```
2019-12-05 11:40:26,177 ERROR [com.ericsson.nms.security.nscs.logger.NscsLog →
ger] (EJB default - 86) [NSCS] : Node [NetworkElement=LTE06dg2ERBS00001] has →
 validation problem.
Exception is [Node does not have supportedKeyAlgorithm attribute under Ntp M →
O]
```

2. that supported MOs for G1 nodes.

Figure 8


```
2019-12-05 13:37:54,567 ERROR [com.ericsson.nms.security.nscs.data.moget.imp
l.CppMOGetServiceImpl] (EJB default - 70)
Node [MeContext=LTE100ERBS00001] doesn't have installedNtpKeyIds attribute u
nder TimeSetting MO.
```

```
2019-12-05 13:37:54,567 ERROR [com.ericsson.nms.security.nscs.logger.NscsLog
ger] (EJB default - 70) [NSCS] : Node [NetworkElement=LTE100ERBS00001] has v
alidation problem.
Exception is [Node does not have installedNtpKeyIds attribute under TimeSett
ing MO]
```

3. Ensure that keys are generated in NTP server.

```
2019-12-05 11:41:27,010 INFO [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-exe
cutor-tp-threads - 424) [NO USER DATA, WorkFlow Task Handler [CppGetNtpKeyDa
taTask], FINISHED_WITH_ERROR, Node Security Service, node [LTE08ERBS00001],
workflow name [CPPNtpConfigure] : workflow id [2b3d718c-1754-11ea-8e23-52540
00b6c87] : CppGetNtpKeyDataTaskHandler:
Exception : class [com.ericsson.oss.services.nscs.workflow.tasks.api.excepti
on.UnexpectedErrorException] : msg [No ntp key details received from ntp ser
vice.]]
```

NTP Configure: the command executes successfully but the response contains "Workflow status" as 'ERROR' and "Workflow Details appear as follows:

Figure 9

4. Verify whether all the preconditions have been met.
5. Verify whether the keyword 'FINISHED_WITH_ERROR' is found at any of the following tasks which indicate NTP configure operation is failed.
   a. Verify whether the CPPInstallNtpKeys has FINISHED_WITH_ERROR message appears in Logviewer.

```
2019-09-06 09:27:43,736 INFO  [com.ericsson.oss.itpf.COMMAND_LOGGER] (j
ob-executor-tp-threads - 3) [NO USER DATA, WorkFlow Task Handler [CppIn
stallNtpKeysTask],
FINISHED_WITH_ERROR, Node Security Service, node [LTE08ERBS00005], work
flow name [CPPInstallNtpKeys] : workflow id [30eb5071-d080-11e9-887a-52
5400219f16] : NtpValidator:
```

```
Maximum Ntp keys limit exceeded on the NodeFdn:MeContext=LTE08ERBS00005
]
```

b. Verify whether the CPPNtpConfigure has FINISHED_WITH_ERROR message appears in Logviewer.

```
2019-09-06 09:30:15,248 INFO  [com.ericsson.oss.itpf.COMMAND_LOGGER] (j
ob-executor-tp-threads - 4) [NO USER DATA, WorkFlow Handler [CPPNtpConf
igure], FINISHED_WITH_ERROR, Node Security Service, node [MeContext=LTE
08ERBS00005], workflow id [89718429-d080-11e9-887a-525400219f16] : Work
flow failed with error com.ericsson.oss.services.nscs.workflow.tasks.ap
i.exception.WorkflowTaskException: CppInstallNtpKeysTaskHandler:
Exception : class [com.ericsson.oss.services.nscs.workflow.tasks.api.ex
ception.WorkflowTaskException] : msg [NtpValidator: Maximum Ntp keys li
mit exceeded on the NodeFdn:MeContext=LTE08ERBS00005] at step CPP NTP C
onfigue with jobID: acfaebcb-f78c-4b81-b75e-e8f06ae079c5 and scheduledW
FID: 8c6c607a-7f40-3e83-acd8-487dc4ccabff]
```

Solution: The maximum NTP keys limit is 10. The user must remove the extra keys from the server with `secadm ntp remove` operation.

c. Verify whether DataAccessException appears in Logviewer.

```
2019-09-27 08:37:29,670 WARN  [com.ericsson.nms.security.nscs.data.moac
tion.MOActionServiceBean](job-executor-tp-threads - 3) Throwing excepti
on because CM returned failure.Reason: cm-writer response -2: Execution
 Error (Node ID: svc-2-mscm. Exception occurred:There is no action name
d TimeSetting::installNtpKeys)
```

```
2019-09-27 08:37:29,671 ERROR [com.ericsson.nms.security.nscs.logger.Ns
csLogger](job-executor-tp-threads - 3) [NSCS] : CppInstallNtpKeysTaskHa
ndler:Exception :class [com.ericsson.nms.security.nscs.api.exception.Da
taAccessException] : msg [Unexpected Internal Error] while performing a
ction: installNtpKeys on:TimeSetting
```

Solution: Ensure all the attributes are present as mentioned in preconditions.

NTP Remove: the execution is successful but the response contains error message that is job finishes with "Workflow status" as 'ERROR' and "Workflow Details appear as follows:

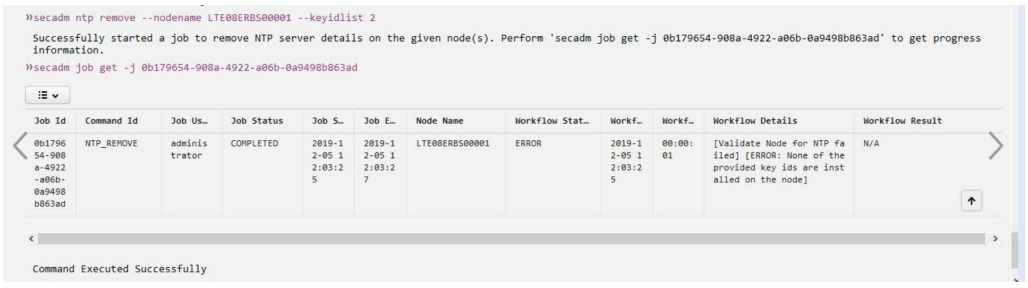


Figure 10

6. Verify whether the keyword 'FINISHED_WITH_ERROR' is found at any of the following tasks which indicate NTP remove operation is failed.

   Verify whether the CPPNtpRemove has FINISHED_WITH_ERROR message appears in Logviewer.

```
2019-09-20 11:44:11,340 INFO  [com.ericsson.oss.itpf.COMMAND_LOGGER] (job-ex
ecutor-tp-threads - 38) [NO USER DATA, WorkFlow Task Handler [ValidateNodeFo
rNtpRemoveTask], FINISHED_WITH_ERROR, Node Security Service, node [RBS548],
workflow name [CPPNtpRemove] : workflow id [9469d5ea-db93-11e9-9415-52540063
56b9] : None of the provided key ids are installed on the node]
```

```
2019-09-24T07:19:05.398+01:00@svc-3-secserv@JBOSS@INFO  [com.ericsson.oss.it
pf.COMMAND_LOGGER] (job-executor-tp-threads - 3) [NO USER DATA, WorkFlow Tas
k Handler [CPPRemoveNtpKeyDataMappingTask], FINISHED_WITH_ERROR, Node Securi
ty Service, node [RBS548], workflow name [CPPNtpRemove] : workflow id [284bb
606-de93-11e9-961a-5254006356b9] : Remove mapping request has been failed on
 node for key Id: 3]
```

Solution: ensure all the keys ids are installed on the nodes.

```
2019-09-24T07:19:05.398+01:00@svc-3-secserv@JBOSS@ERROR [com.ericsson.nms.se
curity.nscs.logger.NscsLogger] (job-executor-tp-threads - 3) [NSCS] : Remove
 mapping request has been failed for node [MeContext=RBS548] and key Id [3]
with status code . [422]
```

```
2019-09-24T07:19:05.398+01:00@svc-3-secserv@JBOSS@INFO  [com.ericsson.oss.it
pf.COMMAND_LOGGER] (job-executor-tp-threads - 3) [NO USER DATA, WorkFlow Tas
k Handler [CPPRemoveNtpKeyDataMappingTask], FINISHED_WITH_ERROR, Node Securi
ty Service, node [RBS548], workflow name [CPPNtpRemove] : workflow id [284bb
606-de93-11e9-961a-5254006356b9] : Remove mapping request has been failed on
 node for key Id: 3]
```

Solution: Check node and key id mapping in data base and ensure removing the mapping in database.

After This Task

If any other issue is found, collect logs of the following Service Groups and db dumps:

- `secserv`
- `itservices`
- `mscmce` for Baseband Nodes
- `mscm` for CPP nodes
- `itservicesdb` dumps

See the section *If Issue Suspected on Node Security* in ENM Data Collection Guidelines, Reference [9], for more details about how to collect respective service group log and db dumps.

See the section Troubleshooting for Configuring NTP Server on page 71 if any error occurs during configuration of NTP server in IT services.

6.14.1 Troubleshooting for Configuring NTP Server

This procedure describes how to troubleshoot the issues that occur during configuring NTP server in IT services.

Prerequisites

— The user has access to the ITServices VM as authorized user.

— Trusted NTP server must be configured and enabled. For detailed information on the Trusted NTP server configuration, see the section *Trusted NTP Server Configuration in ENM* in the document ENM Operators Guide, Reference [3].

— User needs Scripting_Operator role.

Steps

1. Check the logs located in `/var/log/messages` if any error occurs during NTP server configuration.
2. Verify whether keys are updated in both `ntp.conf` file and keys file located in `/etc/ntp.conf` after every successful configuration, if any error occurs during NTP server configuration.
3. Generate NTP keys.

   During the keys generation, if any interruption occurred from the keyboard, execution can stop without completion of the key generation process.

   ```
   Interruption occurred while keys are being generated, please
   wait, while reverting back.....

   Changes have been Successfully reverted
   ```

   Solution: All the added NTP keys are deleted from the database as generation of NTP keys execution interrupted. Then, retry the generation of NTP keys.
4. Add more NTP keys to existing key.

   During the keys generation, if any interruption occurred from the keyboard, execution can stop without completion of the key generation process.

   ```
   Interruption occurred while keys are being generated, please
   wait, while reverting back.....

   Added keys have been successfully reverted as
   KeyBoardInterruption occurred
   ```

Solution: All the added NTP keys are deleted from the database as addition of NTP keys execution interrupted. Then, retry the addition of NTP keys.

5. Replace all the NTP keys.

   During the keys generation, if any interruption occurred from the keyboard, execution can stop without completion of the key generation process.

   ```
   Interruption occurred while keys are being generated, please
   wait, while reverting back.....

   Changes have been Successfully reverted

   Replacing of ntp keys has been failed as KeyBoardInterruption
   occurred
   ```

   Solution: All the existing and generated NTP keys are deleted from the database as replacing action of NTP keys is interrupted. Then, retry the replace NTP keys action.

6. Renew NTP keys.

   Before performing this operation make sure that all the steps are performed or not as described in the procedure. If any one of the steps is missed while performing renew keys operation, the NTP communication fails between ENM and Network Element.

7. Upgrade Server.

   After server upgrade, if nodes trusted NTP time sync fails, then the reason can be the key data in `/etc/ntp/keys` file is lost which resulted in trusted NTP sync failure on node.

   Solution: Configure key data in `/etc/ntp/keys` file in all `itservices vms`, by logging on `itservices` as authorized user and execute the following commands.

   Enable NTP Service:

   ```
   [<authorized_user>@svc-<x>-itservices ~]# /opt/ericsson/itservice/bin/its.py →
    --service enable services=ntp
   ```

   Restart NTP Service:

   ```
   [<authorized_user>@svc-<x>-itservices ~]#sudo service ntpd restart
   ```

6.14.2 Troubleshooting for Configuring the Disable Weak Ciphers

> This procedure describes how to troubleshoot the issues that occur during configuring the weak algorithms.

Note: For CPP based nodes, the ENM has to be upgraded to the same existing version, then only the PIB values are reflected.

6.14.2.1 Troubleshooting for "Failed to connect to TLS channel"

A TLS Communication fails with the following "Failed to connect to TLS channel", if the user unexpectedly disabled all the algorithms in ENM that are supported by the node.

For example, user disabled an algorithm value() that is supported by the node.

```
[root@svc-1-sps cloud-user]# /opt/ericsson/PlatformIntegrationBridge/etc/config.
py update --app_server_address svc-1-sps:8080 --name="disableWeakEncryptionAlgor
ithms" --value="tls:AES_128_CBC"
```

The following error appears:

```
2020-10-28 11:26:54,237 ERROR [com.ericsson.oss.mediation.cba.handlers.netconf.N
etconfConnectHandler] (Thread-164 (HornetQ-client-global-threads-690896212)) com
.ericsson.oss.mediation.cba.handlers.netconf.NetconfConnectHandler$Proxy$_$$_Wel
dSubclass is failed: com.ericsson.oss.mediation.util.netconf.api.exception.Netco
nfManagerException: com.ericsson.oss.mediation.transport.api.exception.Transport
Exception: Failed to connect.
2020-10-28 11:26:54,237 ERROR [com.ericsson.oss.mediation.cba.handlers.netconf.N
etconfConnectHandler] (Thread-164 (HornetQ-client-global-threads-690896212))
>>>>ERROR: com.ericsson.oss.itpf.sdk.core.retry.RetriableCommandException: com.e
ricsson.oss.mediation.util.netconf.api.exception.NetconfManagerException: com.er
icsson.oss.mediation.transport.api.exception.TransportException: Failed to conne
ct.
>>>>ERROR: com.ericsson.oss.mediation.util.netconf.api.exception.NetconfManagerE
xception: com.ericsson.oss.mediation.transport.api.exception.TransportException:
 Failed to connect.
>>>>ERROR: com.ericsson.oss.mediation.transport.api.exception.TransportException
: Failed to connect.
>>>>ERROR: com.ericsson.oss.mediation.adapter.tls.exception.TlsException: TlsExc
eption CAUSE_CODE : Failed to connect to TLS channel (16)
>>>>ERROR: com.ericsson.oss.mediation.adapter.tls.exception.TlsChannelException:
 javax.net.ssl.SSLHandshakeException: Received fatal alert: insufficient_securit
y
>>>>ERROR: javax.net.ssl.SSLHandshakeException: Received fatal alert: insufficie
nt_security
```

Prerequisites

— User has root access to the ENM.

Solution

Steps

1. Check whether the algorithm is supported by the node by using the ENM CLI command and disable the supported weak algorithm.

```
secadm get ciphers --protocol <protocolname> --nodelist NetworkElement=<Netw →
orkElemtName>
```

Results

The connection between the node and ENM is established successfully.

After This Task

if any issue is found, collect the logs and database dumps:

— `mscm` for CPP nodes

— `mscmce` for DG2 nodes

— `msfm`

— `mspm`

— `msap`

— `msnnetlog`

— `lvsrouter`

6.14.2.2 Troubleshooting for "SSH connection failed"

An SSH Communication fails with the following "SSH connection failed", if the user unexpectedly disabled all the algorithms in ENM that are supported by the node.

For example, User disabled an algorithm value() that is supported by the node.

```
[root@svc-2-mscmce cloud-user]# sudo /opt/ericsson/PlatformIntegrationBridge/etc →
/config.py update --app_server_address svc-3-mscm:8080 --name="disableWeakEncryp →
tionAlgorithms" --value="SSH:aes256-ctr+aes192-ctr+aes128-ctr+aes128-cbc+3des-cb →
c"
```

The following error appears:

```
2020-10-30 11:33:02,877 ERROR [com.ericsson.oss.mediation.cba.handlers.netconf.N →
etconfConnectHandler] (Thread-64 (HornetQ-client-global-threads-591032119)) com. →
ericsson.oss.mediation.cba.handlers.netconf.NetconfConnectHandler$Proxy$_$$_Weld →
Subclass is failed: com.ericsson.oss.mediation.util.netconf.api.exception.Netcon →
fManagerException: com.ericsson.oss.mediation.transport.api.exception.TransportE →
xception:
2020-10-30 11:33:02,877 ERROR [com.ericsson.oss.mediation.cba.handlers.netconf.N →
```

```
etconfConnectHandler] (Thread-64 (HornetQ-client-global-threads-591032119))
>>>>ERROR: com.ericsson.oss.itpf.sdk.core.retry.RetriableCommandException: com.e →
ricsson.oss.mediation.util.netconf.api.exception.NetconfManagerException: com.er →
icsson.oss.mediation.transport.api.exception.TransportException:
>>>>ERROR: com.ericsson.oss.mediation.util.netconf.api.exception.NetconfManagerE →
xception: com.ericsson.oss.mediation.transport.api.exception.TransportException:
>>>>ERROR: com.ericsson.oss.mediation.transport.api.exception.TransportException →
:
>>>>ERROR: com.ericsson.oss.mediation.transport.ssh.maverick.provider.exception. →
OpenConnectionException: SSH connection failed
>>>>ERROR: com.maverick.ssh.SshException: Failed to negotiate a transport compon →
ent [aes256-cbc,aes192-cbc,blowfish-cbc,3des-ctr,arcfour,arcfour128,arcfour256] →
[aes256-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-gcm@openssh.com,aes128-ctr, →
AEAD_AES_256_GCM,AEAD_AES_128_GCM,aes128-cbc,3des-cbc] [Unknown cause]
2020-10-30 11:33:02,877 ERROR [com.ericsson.oss.mediation.cba.handlers.netconf.N →
etconfConnectHandler] (Thread-64 (HornetQ-client-global-threads-591032119)) setS →
ocketTimeout failed: 100000
```

Prerequisites

— User has root access to the ENM.

Solution

Steps

1. Check whether the algorithm is supported by the node by using the ENM CLI command and disable the supported weak algorithm.

```
secadm get ciphers --protocol <protocolname> --nodelist NetworkElement=<Netw →
orkElemtName>
```

Results

The connection between the node and ENM is established successfully.

After This Task

if any issue is found, collect the logs and database dumps:

— `mscm` for CPP nodes

— `mscmce` for DG2 nodes

— `msfm`

— `mspm`

— `msap`

— `msnnetlog`

— `lvsrouter`

7 OpenIDM Synchronization Troubleshooting

This task describes symptoms that indicate issues with OpenIDM synchronization and provides steps to collect logs and apply a workaround.

The symptom is:

— It is not possible to log on with newly created user account. The administrator user can be also impacted if the server has been initial installed.

Prerequisites

Root access to the OpenIDM Virtual Machine.

Steps

1. Log on OpenIDM VM as root.

   See the sections *VM Security Tasks* and *Connect to a Virtual Machine* in the ENM System Administration Guide.

   ```
   sudo su -
   ```

   Enter root password.

2. Execute `collectTroubleshootingData.sh` script to collect OpenIDM logs:

   ```
   /ericsson/tmp/openidm/bin/collectTroubleshootingData.sh
   ```

   OpenIDM logs are packed into a `tar.gz/ericsson/log/openidm/` package and directory. Logs must be downloaded and sent to the developer team.

3. Execute following command to restart OpenIDM:

   ```
   service openidm restart
   ```

   Result: Restart takes about a minute. Afterward, it is possible to log on with a newly created account package, and located in.

Results

The logs are collected and create or edit user operations are possible. It is now possible to log on a new user account.

7.1 Openidm Monitor Offline During Upgrade

Sporadic monitor offline events for Openidm VM can happen during Upgrade. The presence of the monitor offline does not impact any functionality and use case in ENM.

8 Workaround for Activation of Security Level 2 Fail for CPP Nodes

This task describes how to switch the CPP Node to security level 2 when trust installation is failed for SFTP `known_hosts` issue.

The symptom is:

— Node does not get switched to SL2 and error related to trust installation failure on node is observed.

It describes how to delete the `known_hosts` file.

The actors are:

Authorized for : PKI_ADMINISTRATOR, Action : execute.

Authorized for : Cmedit_Administrator, Action : execute.

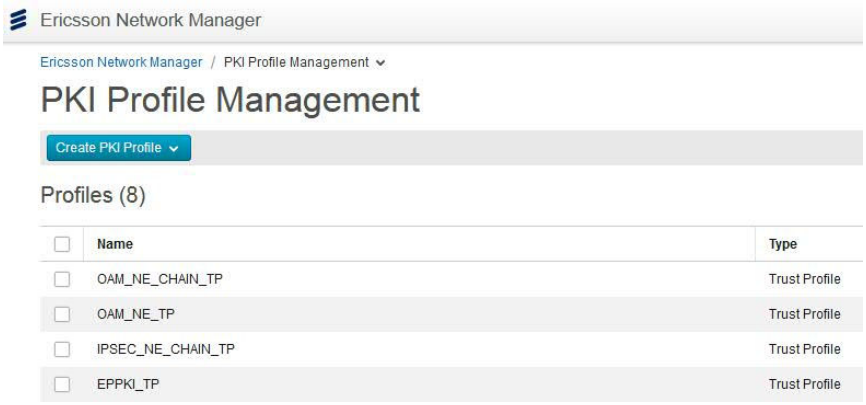
Authorized for : NodeSecurity_Administrator, Action: execute.

Prerequisites

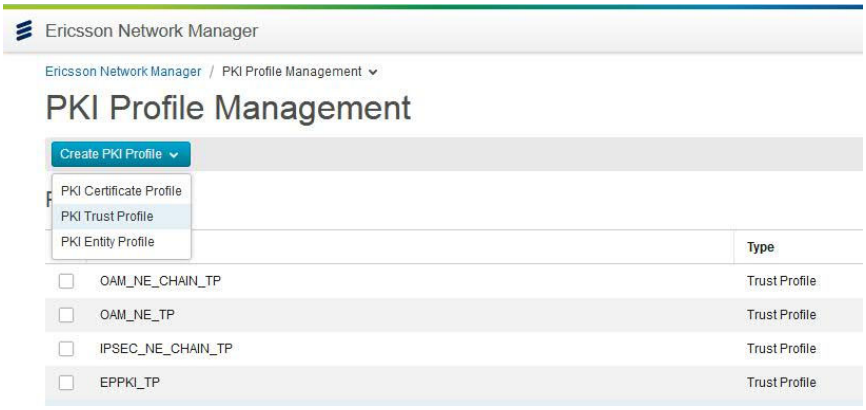
— Node is in sync state.

Steps

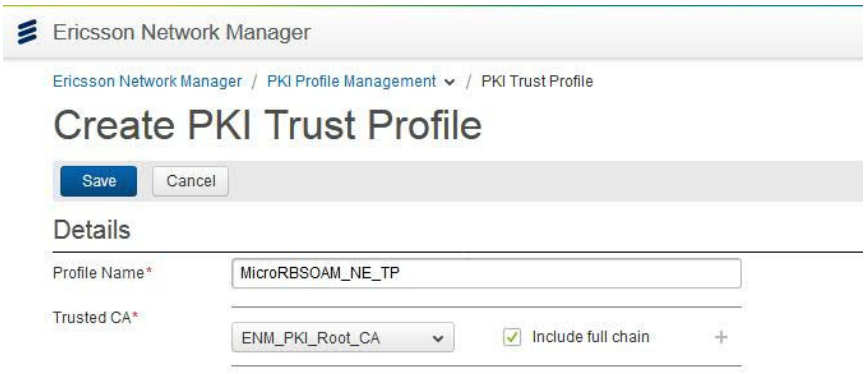
1. Create a TrustProfile.
    a. Go to **PKI Profile Management** application from ENM GUI.



    b. Open and select **PKI Trust Profile**.



c. Give the **Profile Name** as MicroRBSOAM_NE_TP and select **ENM_PKI_CA** from the **Trusted CA** drop-down menu.



d. Select **Save**.

2. Modify the Entity Profile.

   a. Unlock the profile.

      From ENM CLI, run the following command:

      ```
      credm unlock -p MicroRBSOAM_CHAIN_EP -t entity
      ```

   b. Go to **PKI Profile Management** application from ENM GUI.

   c. Select the Entity Profile MicroRBSOAM_CHAIN_EP and click **Edit**.

   d. Clear OAM_NE_CHAIN_TP and select MicroRBSOAM_NE_TP from the trust profile drop-down menu.

   e. Save the profile.

   f. Lock the profile:

```
credm lock -p MicroRBSOAM_CHAIN_EP -t entity
```

3. Delete the known_hosts file.
    a. Log on the node using SSH or AMOS.
    b. Go to the .ssh directory:

    ```
    cd /c/.ssh/
    ```

    c. Remove the known_hosts file:

    ```
     rm known_hosts
    ```

4. Delete the existing Trusted Cert (intermediate file) from node.
    a. Go to /c/security/ directory of the node:

    ```
     cd /c/security/
    ```

    b. Remove all the .der files from the directory:

    ```
    rm <file-name>.der
    ```

5. Cancel the previous trusted certificates installation.
    a. Cancel the reset previous failure if any:

    ```
     cmedit action MeContext=<nodename>,ManagedElement=1,SystemFunction →
    s=1,Security=1 cancelInstallTrustedCertificates
    ```

    b. Sync the node.

    ```
    cmedit action NetworkElement=<node-name>,CmFunction=1 sync
    ```

6. Switch security level.
    a. Switch security level.

    ```
    secadm sl set -l 2 -xf file:<file>.xml
    ```

    b. Confirm the security level status.

    ```
    secadm sl get -n <nodename>
    ```

8.1 Workaround for Certificate Reissue Failure on PICO Real Node

This task describes how to resolve when the reissue (IPSEC/OAM) on the PICO real node fails if it contains NULL values for the MOs enrollmentAuthorityName, enrollmentCaCertificate, and enrollmentCaFingerprint.

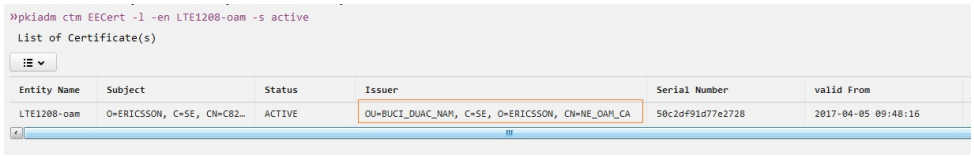
Steps

1. Create the EnrollmentAuthority with the following parameters:

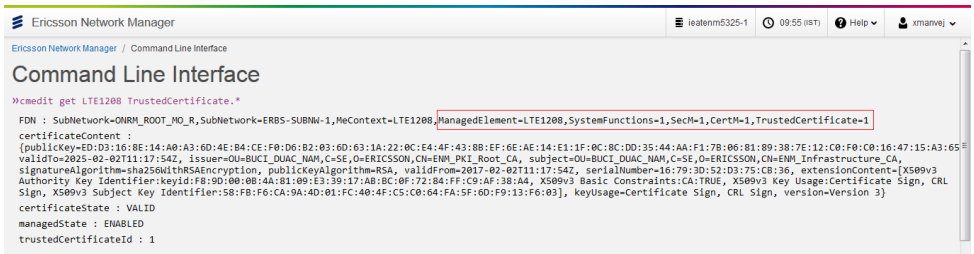
   ```
   enrollmentAuthorityId=3
   ```

   ```
   enrollmentAuthorityName= SubjectDN of Node Issuer CA
   ```

   Example

   enrollmentCaCertificate = Trusted Certificate MO having RA issuer's Root CA certificate

   Example

   ```
   ManagedElement=<NodeName>,SystemFunctions=1,SecM=1,CertM=1,TrustedCertificat
   e=#
   ```

   ```
   enrollmentCaFingerprint= FingerPrint of the RA issuer's Root
   CA certificate.
   ```

   See Workaround for Certificate Reissue Failure on PICO Real Node on page 81 for retrieving the CA fingerprint.

   authorityType = REGISTRATION_AUTHORITY

   ```
   cmedit create <RootMO>,ManagedElement=<NodeName>,SystemFunctions=1,SecM=1,Ce
   rtM=1,EnrollmentAuthority=3 enrollmentAuthorityId=3,enrollmentAuthorityName=
   "<SubjectDN of Node Issuer CA>",enrollmentCaCertificate="<Trusted Certificat
   e having RA issuer's Root CA certificate>",enrollmentCaFingerprint="<FingerP
   ```

```
rint of the RA issuer's Root CA certificate>",authorityType="REGISTRATION_AU →
THORITY"
```

2. Set the created EnrollmentAuthority to EnrollmentServerGroup.

```
cmedit set <RootMO>,ManagedElement=<NodeName>,SystemFunctions=1,SecM=1,CertM →
=1,EnrollmentServerGroup=1,EnrollmentServer=1 enrollmentAuthority="<RootMO>, →
ManagedElement=<NodeName>,SystemFunctions=1,SecM=1,CertM=1,EnrollmentAuthori →
ty=3"
```

3. Delete the existing EnrollmentAuthority.

```
cmedit delete <RootMO>,ManagedElement=<NodeName>,SystemFunctions=1,SecM=1,Ce →
rtM=1,EnrollmentAuthority=1 --force
```

4. Perform the Online Certificate Enrollment Reissue.

```
secadm cert issue -ct OAM/IPSEC -xf file:<xml_file_name>
```

8.1.1 Retrieve CA Fingerprint for RA Issuer Root CA Certificate

> This section describes the method to obtain fingerprint for RootCA certificate in the RA certificate chain.

Actors

— Authorized for: PKI_ADMINISTRATOR, Action : execute

Prerequisites

— Access to Linux environment with openssl

Note: CA Name is the RootCA in the RA certificate chain.

Steps

1. Download Root CA certificate.
   — If the Root CA is ENM CA perform step 2.
   — If the Root CA is External CA perform step 3.
2. Download the ENM Root CA certificate:

```
pkiadm certmgmt CACert -expcert -en <CA Name> -f PEM
```

3. Download the External Root CA certificate.

a. Obtain the issuer of the NE_IPsec_Operator_CA/ENM_PKI_Root_CA which is external CA:

```
pkiadm ctm CACert -l -en NE_IPsec_Operator_CA -s activ
e
```

Example

```
»pkiadm ctm CACert -l -en NE_IPsec_Operator_CA -s active
List of Certificate(s)
Entity Name          Subject                                                    Status  Issuer
NE_IPsec_Operator_CA O=ERICSSON, C=SE, OU=BUCI_DUAC_NAM, CN=NE_IPsec_Operator_CA ACTIVE  O=TCS, C=IN, OU=DLF, CN=PrimeTowerIntermediateCA
```

Note the issuer from the active certificate of NE_IPsec_Operator_CA.

b. Obtain the external CA list using the command:

```
pkiadm extcalist
```

Verify whether the subject of the listed External CAs is similar to the IssuerDN from step a and note the **External CA Name**.

```
»pkiadm extcalist
List of Certificate(s)
External CA Name          Subject                                    Issuer
ExternalIntermediateCA    O=TCS, C=IN, OU=DLF, CN=PrimeTowerIntermediateCA O=TCS, C=IN, OU=DLF, CN=PrimeTowerRootCA
VC_Root_CA_A1             CN=VC_Root_CA_A1, O=Ericsson, C=SE         CN=VC_Root_CA_A1, O=Ericsson, C=SE
ExternalRootCA            O=TCS, C=IN, OU=DLF, CN=PrimeTowerRootCA   O=TCS, C=IN, OU=DLF, CN=PrimeTowerRootCA
```

Obtain the chain of External CAs by validating the issuer and the subject and note the **External CA Name**

```
»pkiadm extcalist
List of Certificate(s)
External CA Name          Subject                                    Issuer
ExternalIntermediateCA    O=TCS, C=IN, OU=DLF, CN=PrimeTowerIntermediateCA O=TCS, C=IN, OU=DLF, CN=PrimeTowerRootCA
VC_Root_CA_A1             CN=VC_Root_CA_A1, O=Ericsson, C=SE         CN=VC_Root_CA_A1, O=Ericsson, C=SE
ExternalRootCA            O=TCS, C=IN, OU=DLF, CN=PrimeTowerRootCA   O=TCS, C=IN, OU=DLF, CN=PrimeTowerRootCA
```

c. Download the External Root CA certificate.

```
pkiadm extcaexport --name <External CA Name> --serialnumber <Serial
 Number>
```

4. Retrieve the CA Fingerprint.

```
openssl x509 -in <path>/file.pem -sha1 -noout -fingerprint
```

Execute this command on any Linux environment that has openssl.

Results

CA Fingerprint must be obtained for ENM/External RootCA certificate in the RA certificate chain.

9 Troubleshooting Node Up Notification Waiting During AP Zero Touch

During Baseband node AP zero touch, node UP notification is stuck at `waiting state`. One of the reasons for this is that node time is not in sync with ENM time.

Prerequisites

— Root access to Node.

— Root access to LMS.

— Credm_Administrator, PKI_Administrator Roles.

Steps

1. Check current time on node.

   Log on the node and navigate to: `ManagedElement=<<nodename>>, SystemFunctions=1, SysM=1, TimeM=1, DateAndTime=1` for current date of node.

2. Check the time on ENM.

   Log on master server using root credentials and execute the following command:

   ```
   [root@cloud-ms-1 ~]# date
   Tue May 30 07:03:10 IST 2017
   ```

   If there is a discrepancy in both the dates, the time on node needs to be synced with the ENM time. Steps 3–6 are workaround for the node to install the certificate.

3. Unlock the certificate profile.

   Refer to default profile names from the table.

   ```
   credm unlock -p <<profile_name>> -t certificate
   ```

Node	Certificate Profile
Pico	OAM: PicoRBSOAM_RS_SAN_CP IPsec: PicoRBSIPSec_RS_SAN_CP
CPP	OAM: MicroRBSOAM_CP IPsec: MicroRBSIPSec_SAN_CP
G2/BB	OAM: DUSGen2OAM_CP IPsec: DUSGen2IPSec_SAN_CP

4. Change Skew Certificate time (in minutes) to be inline with the node time. Calculate the time difference (in minutes) between ENM (step 2) and Node (step 1) and set it to Skew Certificate time.

5. Lock certificate profile.

```
credm lock -p <<profile_name>> -t certificate
```

6. Re-execute the use-case.

10 Recovery Procedure for Naming Conflict on Cloud for M2Musers

In a scenario where a M2MUser is not able to log on, verify if it is a replication naming conflict.

It can happen when changes to the same entry are applied to multiple OpenDJ servers at the same time.

Prerequisites

administrator password for OpenDJ.

Steps

1. Connect to each OpenDJ instance and check duplicated entries.

   The following example is reported for entry with `uid=<mm-software>,ou=<M2MUsers>,dc=<ieatenmc5a01-10>,dc=<com>` with different passwords.

   ```
   Connect to opendj-1 VM and execute the following command:

   [root@opendj-1~]/ericsson/opendj/opendj/bin/ldapsearch -p 1636 --useSSL --tr →
   ustAll -D "cn=directory manager" -w <ldap_admin_password> -b "uid=mm-softwar →
   e,ou=M2MUsers,$(grep COM_INF_LDAP_ROOT_SUFFIX /ericsson/tor/data/global.prop →
   erties | cut -d '=' -f 2-)" objectclass=*
   ```

   Expected Result:

   ```
   dn: uid=mm-software,ou=M2MUsers,dc=ieatenmc5a01-10,dc=com

   objectClass: person
   objectClass: inetorgperson

   objectClass: posixAccount
   objectClass: organizationalPerson

   objectClass: top
   gidNumber: 5000

   uid: mm-software
   userPassword: {SSHA256}VydH/GN6lGNAL4O8YIL+ku+nVnggzUG07odd5r/B05sA7aZZjjeBw →
   g==

   sn: mm-software
   authPassword: SHA1$AESCBC128$Kz3muuvo0OukhpGEk+ZP35aavBgn9LbhWeK2yWnhWTQ=

   cn: mm-software
   loginShell: /sbin/nologin

   homeDirectory: /home/smrs/smrsroot/software/erbs/ uidNumber: 20001
   ```

2. Connect to opendj-2 VM and execute the following command:

```
[root@opendj-2~]/ericsson/opendj/opendj/bin/ldapsearch -p 1636 --useSSL --tr
ustAll -D "cn=directory manager" -w <ldap_admin_password> -b "uid=mm-softwar
e,ou=M2MUsers,$(grep COM_INF_LDAP_ROOT_SUFFIX /ericsson/tor/data/global.prop
erties | cut -d '=' -f 2-)" objectclass=*
```

Expected Result:

```
dn: uid=mm-software,ou=M2MUsers,dc=ieatenmc5a01-10,dc=com
objectClass: person
objectClass: inetorgperson
objectClass: posixAccount
objectClass: organizationalPerson
objectClass: top
gidNumber: 5000
uid: mm-software
userPassword: {SSHA256}TKe8Vpg50+ApF/7dw8v2fouxgA+3ms7du1FrjF3XuzsjeNLDz6yGZ
g==
sn: mm-software
authPassword: SHA1$AESCBC128$WzQAQTBC3TSIQNviAykcNt4UoN2BZpMvXhZ00F4EkWg=
cn: mm-software
loginShell: /sbin/nologin
homeDirectory: /home/smrs/smrsroot/software/erbs/
uidNumber: 20001

dn: entryuuid=2dc6cb05-c27f-4acb-a25c-18da5c4c8b1f+uid=mm-software,ou=M2MUse
rs,d
c=ieatenmc5a01-10,dc=com
objectClass: person
objectClass: inetorgperson
objectClass: posixAccount
objectClass: organizationalPerson
objectClass: top
uid: mm-software
gidNumber: 5000
sn: mm-software
userPassword: {SSHA256}VydH/GN6lGNAL4O8YIL+ku+nVnggzUG07odd5r/B05sA7aZZjjeBw
g==
authPassword: SHA1$AESCBC128$Kz3muuvo0OukhpGEk+ZP35aavBgn9LbhWeK2yWnhWTQ=
cn: mm-software
loginShell: /sbin/nologin
homeDirectory: /home/smrs/smrsroot/software/erbs/
uidNumber: 20001
```

The entry: dn: entryuuid=*<2dc6cb05-c27f-4acb-a25c-18da5c4c8b1f+>*uid=*<mm-software>*,ou=*<M2MUsers>*,dc=*<ieatenmc5a01-10>*,dc=*<com>* is created by OpenDJ replication task when it finds a naming conflict in the two OpenDJ instances.

Step to recover the replication naming conflict:

3. Connect to the opendj instance where the "wrong" entry is present (generally this is the entry with the oldest modification) and then remove the entry using the following command:

```
[root@opendj-1~]#/ericsson/opendj/opendj/bin/ldapdelete -p 1636 --useSSL --t
rustAll -D "cn=directory manager" -w <ldap_admin_password> "uid=mm-software,
ou=M2MUsers,$(grep COM_INF_LDAP_ROOT_SUFFIX /ericsson/tor/data/global.proper
ties | cut -d '=' -f 2-)"
```

11 Troubleshooting for FTPES Supported Use Cases

This section is applicable for trouble shooting the failures in FTPES supported usecases like SHM Upgrade and Backup software, Netlog download, Amos Logs download and Upgrade Independence.

If any of the above usecase is failed with the FTPES enabled Network Elements, the following sections need to be executed to confirm the issue is not with the blocking of ports.

11.1 Check Enabled Port in Firewalls Between ENM and Network Elements

> Check if the followings ports are enabled in firewalls (If any) between ENM and Network Elements.

1. 9921 and 32768–40999 (Network Element Ports) for FTPES outgoing connections from ENM to Network Elements
2. 9921 (ENM port) for FTPES incoming connections from Network Element to ENM

If any of the above ports are not enabled, then enable the same in the Firewalls between ENM and Network Elements.

11.2 Check and Enabling Ports in Physical Environment

This section describes the procedure for:

— The verification and enabling of 9921 port in iptables.

— The verification and addition of IPv4 and IPv6 NAT for 9921 port.

Steps

1. Verify and enable of FTPES port in iptables in all LVS Router VMs.

```
STEPS TO VERIFY IF 9921 ARE ENABLED IN IPTABLES FOR PHYSICAL ENVIRONMENT.
1.Login to ms-1
2.Login to lvsrouter VM
3.Execute "sudo su" command for root privileges.
4.Execute "iptables -L | grep 9921" to verify if 9921 port is opened in iptables.
5.If 9921 port is not opened in iptables, Execute below commands
  Example commands:
```

```
   For IPV4 execute "iptables -A FORWARD -i eth2 -o eth0 -p tcp -m tcp --dport 9921 -j ACCEPT";
   For IPV6 execute "ip6tables -A FORWARD -i eth2 -o eth0 -p tcp -m tcp --dport 9921 -j ACCEPT";
```

2. Verify and add of IPv4 and IPv6 NAT for FTPES port in all LVS Router VMs.

```
STEPS TO VERIFY and ADD IPv4/IPv6 NAT for 9921 port IN PHYSICAL ENVIRONMENT.
1.Login to ms-1
2.Login to lvsrouter VM
3.Execute "sudo su" command for root privileges.
4.Execute "ipvsadm -Ln | grep 9921" to verify 9921 NAT.
6.The result shoud show routing configuration to all available SMRS Real IPs. If the result does n →
ot show Ipv4 and Ipv6 routing for 9921 port,
  Follow below procedure to collect CM vip ipaddress and smrs real ipaddress.
  6.1 a.To collect CM vip ipaddress:
      b.Execute : grep -e vip /ericsson/tor/data/global.properties
      c.Collect svc_CM_vip_ipaddress
      d.Collect svc_CM_vip_ipv6address
  6.2 a.To collect smrs real ipv4 address
      b.cat /etc/hosts | grep smrs
      c.Collect smrs Real IPV4 Addresses
  6.3 a.To collect smrs real ipv6 address
      b.Login to smrsserv.
      c.Execute "ifconfig"
      d.Collect inet6 smrs address of global scope.
7.If Ipv4 or Ipv6 NAT is not present for 9921 port,
  Follow below commands to add IPv4/IPv6 NAT for 9921 port.
  7.1 IPv4 NAT Example: ipvsadm -A -t <svc_CM_vip_ipaddress>:9921 -s lc
                        ipvsadm -a -t <svc_CM_vip_ipaddress>:9921 -r <SMRS Real IPv4 Address1>:992 →
1 -m
                        ipvsadm -a -t <svc_CM_vip_ipaddress>:9921 -r <SMRS Real IPv4 Address2>:992 →
1 -m
  7.2 IPv6 NAT Example: ipvsadm -A -t <svc_CM_vip_ipv6address>:9921 -s lc
                        ipvsadm -a -t <svc_CM_vip_ipv6address>:9921 -r <SMRS Real IPv6 Address1>:9 →
921 -m
                        ipvsadm -a -t <svc_CM_vip_ipv6address>:9921 -r <SMRS Real IPv6 Address2>:9 →
921 -m
 9.Execute "ipvsadm -Ln | grep 9921" to verify 9921 NAT.
```

11.3 Check and Enable the FTPES Port (9921) in Cloud Environment

This section describes the procedure for:

— The verification and enabling of 9921 in iptables.

— The verification and addition of IPv4 and IPv6 NAT for 9921 port.

Steps

1. Verify and enable of 9921in iptables.

```
STEPS TO VERIFY IF 9921 is ENABLED IN IPTABLES FOR CLOUD ENVIRONMENT.
1.Login to vnflaf
2.Login to lvsrouter VM
3.Execute "sudo su" command for root privileges.
4.Execute "iptables -L | grep 9921" to verify if 9921 port is opened in iptables.
5.If 9921 port is not opened in iptables, Execute below commands
  Example commands:
   For IPv4 execute "iptables -A FORWARD -i eth1 -o eth0 -p tcp -m tcp --dport 9921 -j ACCEPT";
   For IPv6 execute "ip6tables -A FORWARD -i eth1 -o eth0 -p tcp -m tcp --dport 9921 -j ACCEPT";
```

2. Verify and add of IPv4 and IPv6 NAT for FTPES port in all LVS Router VMS.

```
STEPS TO VERIFY and ADD IPv4/IPv6 NAT FOR 9921 PORT IN CLOUD ENVIRONMENT.
1.Login to vnflaf
2.Login to lvsrouter VM
3.Execute "sudo su" command for root privileges.
4.Execute "ipvsadm -Ln | grep 9921" to verify 9921 NAT.
5.If Ipv4 or Ipv6 NAT is not present for 9921 port,
  Follow below procedure to collect CM vip ipaddress and smrs real ipaddress.
  5.1 a.To collect CM vip ipaddress:
      b.Execute : consul kv get -recurse | grep "global"
      c.Collect svc_CM_vip_ipaddress
      d.Collect svc_CM_vip_ipv6address
  5.2 a.To collect smrs real ipv4 address
      b.consul members | grep smrs
      c.Collect smrs Real IPV4 Addresses
  5.3 a.To collect smrs real ipv6 address
      b.Login to smrsserv.
      c.Execute "ifconfig"
      d.Collect inet6 smrs address of global scope.
6.If Ipv4 or Ipv6 NAT is not present for 9921 port,
  Follow below commands to add IPV4/IPV6 NAT for 9921 port.
  6.1 IPv4 NAT Example: ipvsadm -A -t <svc_CM_vip_ipaddress>:9921 -s lc
                        ipvsadm -a -t <svc_CM_vip_ipaddress>:9921 -r <SMRS Real IPV4 Address1>:992 →
1 -m
                        ipvsadm -a -t <svc_CM_vip_ipaddress>:9921 -r <SMRS Real IPV4 Address2>:992 →
1 -m
  6.2 IPv6 NAT Example: ipvsadm -A -t <svc_CM_vip_ipv6address>:9921 -s lc
                        ipvsadm -a -t <svc_CM_vip_ipv6address>:9921 -r <SMRS Real IPV6 Address>:99 →
21 -m
                        ipvsadm -a -t <svc_CM_vip_ipv6address>:9921 -r <SMRS Real IPV6 Address>:99 →
21 -m
7.Execute "ipvsadm -Ln | grep 9921" to verify 9921 NAT.
```

11.4 In Cloud Environment Openstack Security Rules Required for an ENM on Cloud Deployment for 9921 Port

This section describes the procedure to add openstack security rules in Cloud deployments for 9921 port.

Do the following steps for opening security group rules:

Steps

1. Log on the client machine and set the environment with the `keystonerc` file.
2. Check what rules are present by issuing the following command, for both Internal and External security groups.

```
# openstack security group rule list <enm_external_security_group_name> | grep <port>
```

Example

For example, to list the port "9921" traffic run the follwoing command.

```
# openstack security group rule list <enm_external_security_group_name> | gr →
ep 9921
```

3. If 9921 rule is not present in the applied security group, then add IPv4 and IPv6 addresses as follows:

```
# openstack security group rule create \
--<ingress|egress> \
--ethertype <IPv4|IPv6> \
--protocol <protocol> \
--dst-port <port:port> \
--src-ip <remote ip or group> \
<security group name>
```

Example

For example, to add a new port "9921" for TCP ingress traffic from any source IPv4 address run the following:

```
# openstack security group rule create \
--ingress \
--ethertype IPv4 \
--protocol tcp \
--dst-port 9921:9921\
--src-ip 0.0.0.0/0\
enm_external_security_group
```

For example, to add a new port "9921" for TCP ingress traffic from any source IPv6 address run the following:

```
# openstack security group rule create \
--ingress \
--ethertype IPv6 \
--protocol tcp \
--dst-port 9921:9921\
--src-ip ::/0\
enm_external_security_group
```

4. Run the following command to ensure that the new rules have been applied for both External security groups.

```
# openstack security group rule list <enm_external_security_group_name> | grep <port added>
```

12 Troubleshooting OpenDJ

Use this section to troubleshoot issues that occur with OpenDJ.

If there are problems with OpenDJ:

Steps

On Physical Environment

1. Run the `ldapsearch` command (or another `ldapsearch` command from *List the Contents of the OpenDJ LDAP Database* section in ENM System Administrator Guide, Reference [1] to check if OpenDJ connects to the database, and check if it returns the "Connect Error" message:

   ```
   # /opt/opendj/bin/ldapsearch -p 1636 --useSSL --trustAll -D "cn=directory ma →
   nager" -w ldap_password -b "" objectclass=* | grep uid:
   Connect Error
   Result Code:  91 (Connect Error)
   ```

   If OpenDJ connects to the database correctly, the `ldapsearch` command returns the list from the database:

   ```
   [root@ieatrcxb3211 litp-admin]# /opt/opendj/bin/ldapsearch -p 1636 --useSSL  →
   --trustAll -D "cn=directory manager" -w ldap_password -b "" objectclass=* |  →
   grep uid:
   uid: administrator
   uid: ENMuser
   uid: com_user
   uid: temporary_user
   ...
   ```

2. On Physical environment, verify OpenDJ status using the `hagrp` and `service opendj status` commands.

   On Cloud environment, verify the OpenDJ status using the `consul members` and `service opendj status` commands.

3. Check the database status using the status command.

4. Check the OpenDJ logs located in `/var/log/opendj` and in `var/ericsson/log/opendj`.

5. If one DataBase node was down longer than the period set by the `Replication Purge Delay` parameter, see the guidelines in *OpenDJ Recovery when Replication Purge Delay is Exceeded* section in ENM System Administrator Guide, Reference [1].

On Cloud Environment

6. To log on OpenDJ VM, see the sections *VM Security Tasks* and *Connect to a Virtual Machine* in ENM System Administrator Guide, Reference [1]

7. Run the following `ldapsearch` command (or another `ldapsearch` command from *List the Contents of the OpenDJ LDAP Database* section in ENM System Administrator Guide, Reference [1] to check if OpenDJ connects to the database, and check if it returns the "Connect Error" message:

```
/ericsson/opendj/opendj/bin/ldapsearch -p 1636 --useSSL --tru →
stAll -D "cn=directory manager" -w ldap_password -b "" object →
class=* | grep uid:Connect Error
Result Code:  91 (Connect Error)
```

   If OpenDJ connects to the database correctly, the `ldapsearch` command returns the list from the database:

```
/ericsson/opendj/opendj/bin/ldapsearch -p 1636 --useSSL --trustAll -D "cn=directory manager" -w ld →
ap_password -b "" objectclass=* | grep uid:uid: administratoruid: ENMuseruid: com_useruid: tempora →
ry_user...
```

8. Log off from OpenDJ VM and verify OpenDJ status by using the "consul members" command

9. Log on OpenDJ VM and verify OpenDJ status using the `service opendj status` command.

10. Check the database status using the `status` command.

11. Check the OpenDJ logs located in `/var/log/opendj` and in `var/ericsson/log/opendj`.

12. If one DB node was down longer than the period set by the `Replication Purge Delay` parameter, see the guidelines in *OpenDJ Recovery when Replication Purge Delay is Exceeded* section in ENM System Administrator Guide, Reference [1].

13 Troubleshooting COM-AA

This section provides the troubleshooting steps recommended to diagnose and fix common problems in COM-AA

13.1 Check Proxy Agent in Case of Problems with "bind" Operations

Check the proxy agent and used password if you encounter problems with bind operations.

Verify that the credentials used during "bind" operations are valid.

Prerequisites:

— Access to the DB nodes.

— ADMINISTRATOR role required to access the Command Line Interface (CLI) in ENM.

Steps

1. Select **Command Line Interface** in the ENM **Application Launcher**.
2. Run the following ENM CLI command.

```
secadm ldap configure --manual
```

Example

```
»secadm ldap configure --manual

 PROPERTY                        VALUE

 fallbackLdapIpv6Address

 ldapIpv6Address

 tlsPort                         1389

 ldapIpv4Address                 141.137.211.41

 fallbackLdapIpv4Address         141.137.211.42

 ldapsPort                       1636

 bindDn                          cn=ProxyAccount_1,ou=proxyagent,ou=com,dc=ieatclvmlms904,dc=com

 baseDn                          dc=ieatclvmlms904,dc=com

 bindPassword                    wuo08qpz


 Command Executed Successfully
```

3. Log on any DB node.
4. Perform `ldapsearch` to verify the credentials.

   Use the `bindDN` and `bindPassword` values collected in step 2 using the `secadm` command.

   Example

   ```
   /opt/opendj/bin/ldapsearch -p 1636 --useSSL --trustAll -D "cn=ProxyAccount_1 →
   ,ou=proxyagent,ou=com,dc=ieatclvmlms904,dc=com" -w wuo08qpz -b "ou=people,$( →
   grep COM_INF_LDAP_ROOT_SUFFIX /ericsson/tor/data/global.properties | cut -d →
   '=' -f 2-)" userType=*
   ```

   In this example, `bindDN` is `"cn=ProxyAccount_1,ou=proxyagent,ou=com,dc=ieatclvmlms904,dc=com"` and `bindPassword` is `"wuo08qpz"`

   Replace these values with the ones that reflect your environment.

   Example

   Valid Credentials

   If the credentials are valid, a list of users is displayed:

   ```
   [root@ieatrcxb5160 litp-admin]# /opt/opendj/bin/ldapsearch -p 1636 --useSSL →
   --trustAll -D "cn=ProxyAccount_5,ou=proxyagent,ou=com,dc=ieatlms4935,dc=com" →
    -w gls37epz -b "ou=people,$(grep COM_INF_LDAP_ROOT_SUFFIX /ericsson/tor/dat →
   a/global.properties | cut -d '=' -f 2-)" userType=*

   dn: uid=administrator,ou=People,dc=ieatlms4935,dc=com
   objectClass: person
   objectClass: userTypeOC
   objectClass: inetOrgPerson
   objectClass: posixAccount
   objectClass: organizationalPerson
   ```

```
objectClass: top
gidNumber: 5004
uid: administrator
mail: security@administrator.com
sn: admin
cn: administrator
givenName: security
roleTG: ADMINISTRATOR:ALL,SECURITY_ADMIN:ALL
loginShell: /bin/bash
userType: enmUser
homeDirectory: /home/shared/administrator
uidNumber: 5000

dn: uid=FM_SETUP_2016-10-18_21-29-48-1152_USER_0,ou=People,dc=ieatlms4935,dc →
=com
objectClass: person
objectClass: userTypeOC
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: top
uid: FM_SETUP_2016-10-18_21-29-48-1152_USER_0
mail: FM_SETUP_2016-10-18_21-29-48-1152_USER_0@ericsson.com
sn: FM_SETUP_2016-10-18_21-29-48-1152_USER_0
cn: FM_SETUP_2016-10-18_21-29-48-1152_USER_0
roleTG: FM_Administrator:ALL
givenName: FM_SETUP_2016-10-18_21-29-48-1152_USER_0
userType: enmUser
...
```

Example

Invalid Credentials

If the credentials are invalid, the following is displayed:

```
[root@ieatrcxb4376-1 litp-admin]# /opt/opendj/bin/ldapsearch -p 1636 --useSS →
L --trustAll -D "cn=ProxyAccount_2,ou=proxyagent,ou=com,dc=ieatclvmlms904,dc →
=com" -w pmp27ylo -b "ou=people,$(grep COM_INF_LDAP_ROOT_SUFFIX /ericsson/to →
r/data/global.properties | cut -d '=' -f 2-)" userType=*
The simple bind attempt failed
Result Code:  49 (Invalid Credentials)
```

13.2 Problems with Missing COM Roles

Perform the steps if you determine that you are missing COM roles and need to create them.

Steps

1. Check the list of predefined COM roles in ENM:
   - SystemAdministrator
   - SystemSecurityAdministrator
   - SystemReadOnly
   - ENodeB_Application_Administrator
   - ENodeB_Application_SecurityAdministrator
   - ENodeB_Application_User

- RBS_Application_Operator
- Support_Application_Administrator
- Support_Application_User
- NodeB_Application_User
- NodeB_Application_Administrator
- EricssonSupport

2. If the required COM role is not in the list of the predefined roles, Security Administrator can create new roles using the Role Management application in ENM.

14 Federated Identity Management Troubleshooting

This section provides the troubleshooting steps recommended to diagnose and fix common problems in the ENM Federated Identity Management Security service.

14.1 Troubleshooting Federated Identity Management Interface (Ericsson Only)

This section contains troubleshooting-purpose Federated Identity Management NBI REST API.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

14.1.1 Set Federated Identity Synchronization Operational State (Ericsson Only)

This REST endpoint is used to set the operational state of the Federated Identity Synchronization internal state machine.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Table 3

Description	Method	Path
Set operational state of federated identity synchronization	PUT	/oss/fidm/sync/operstate

14.1.2 Get Federated Identity Synchronization Additional Parameters (Ericsson Only)

> This REST endpoint is used to get the Federated Identity Synchronization configurable additional parameters.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Table 4

Description	Method	Path
Get federated identity synchronization additional parameters	GET	/oss/fidm/sync/additionalparams

14.1.3 Set Federated Identity Synchronization Additional Parameters (Ericsson Only)

> This REST endpoint is used to set some Federated Identity Synchronization additional parameters.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Table 5

Description	Method	Path
Set federated identity synchronization additional parameters	PUT	/oss/fidm/sync/additionalparams

14.1.4 Create PostgreSQL entry used by Federated Identity Synchronization Application (Ericsson Only)

> This REST endpoint is used to create an entry in PostgreSQL DB used by Federated Identity Synchronization application.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Table 6

Description	Method	Path
Create PostgreSQL entry used by Federated Identity Synchronization Application	POST	/oss/idm/config/idmappl/createappl

14.1.5 Update PostgreSQL entry used by Federated Identity Synchronization Application (Ericsson Only)

> This REST endpoint is used to update an entry in PostgreSQL DB used by Federated Identity Synchronization application.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Table 7

Description	Method	Path
Update PostgreSQL entry used by Federated Identity Synchronization Application	POST	/oss/idm/config/idmappl/updateappl

14.1.6 Delete PostgreSql entry used by Federated Identity Synchronization Application (Ericsson Only)

> This REST endpoint is used to delete an entry in PostgreSql DB used by Federated Identity Synchronization application.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Table 8

Description	Method	Path
Delete PostgreSql entry used by Federated Identity Synchronization Application	DELETE	/oss/idm/config/idmappl/deleteappl

14.1.7 Get All PostgreSQL entries used by Federated Identity Synchronization Application (Ericsson Only)

> This REST endpoint is used to get all entries from PostgreSQL DB used by Federated Identity Synchronization application.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Table 9

Description	Method	Path
Get all PostgreSQL entries used by Federated Identity Synchronization Application	GET	/oss/idm/config/idmappl/getall

14.1.8 Get Single PostgreSQL entries used by Federated Identity Synchronization Application (Ericsson Only)

> This REST endpoint is used to get single entry from PostgreSQL DB used by Federated Identity Synchronization application.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Table 10

Description	Method	Path
Get single PostgreSQL entry used by Federated Identity Synchronization Application	GET	/oss/idm/config/idmappl/getapp/{appname}

14.1.9 Get Availability Module Internal State (Ericsson Only)

> This REST endpoint is used to get internal state of the availability module, responsible to manage communications toward PostgreSql server.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Table 11

Description	Method	Path
Get Availability Module Internal State	GET	/oss/fidm/extidpconfig/getstate

14.1.10 Test Internal Ldap Module (Ericsson Only)

> This REST endpoint is used to test internal ldap module used by Federated Identity Synchronization application.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Table 12

Description	Method	Path
Test Internal Ldap Module	GET	/oss/fidm/extidpldap/idpLdapTest/{providertype}

14.1.11 Test Internal Ldap Module with Paging (Ericsson Only)

> This REST enpoint tests internal LDAP module with page size as additional parameter.

Disclaimer

These REST endpoints are meant only to be used by Ericsson support personnel and can be changed or removed without any prior notification.

Required Security Role

SECURITY_ADMIN

REST Endpoint

Table 13

Description	Method	Path
Test Internal Ldap Module with Paging	GET	/oss/fidm/extidpldap/idpLdapTestPaging/{providertype}/{pagesize}

14.2 Federated Identity Synchronization Troubleshooting

This section provides the troubleshooting steps recommended to diagnose and fix common problems in Federated Identity Synchronization application, running on instances of `idmserv` service group and responsible for performing the federated users synchronization from an External Identity Provider (External IdP) to the ENM Local Identity Provider (Local IdP).

14.2.1 Synchronization REST Failed with "httpStatusCode" : 403, "userMessage" : "The User does not have permissions to perform this action."

Prerequisites

— User has mandatory roles: SECURITY_ADMIN.

— User executes command from UI or NBI.

Cause

User executing the sync REST does not have the SECURITY_ADMIN privilege (unsatisfied prerequisite).

Recommendation or Workaround

The user must have the SECURITY_ADMIN privilege assigned to the user performing the sync REST.

14.2.2 Synchronization REST Failed with "httpStatusCode" : 403, "userMessage" : "The User does not have permissions to perform this action."

Prerequisites

— User has mandatory roles: SECURITY_ADMIN.

— User executes command from UI or NBI.

Cause

User executing the sync REST does not have the SECURITY_ADMIN privilege (unsatisfied prerequisite).

Recommendation or Workaround

The user must have the SECURITY_ADMIN privilege assigned to the user performing the sync REST.

14.2.3 Synchronization REST Failed with "httpStatusCode": 422, "userMessage":"External IdP synchronization is still initializing."

Prerequisites

— User has mandatory roles: SECURITY_ADMIN.

— User executes command from UI or NBI.

Cause

The REST is started while the Federated Identity Synchronization application (running on `idmserv` Service Group) is not able to connect to the Generic Identity Configuration (GIC) application (running on `secserv` Service Group). GIC provides access to PostgreSQL database containing the persistent configuration data of Federated Identity Synchronization application.

This condition can be verified performing the get of the synchronization state (see the section *Get Federated Identity Synchronization State* in the document ENM System Security Configuration Programmers Guide, Reference [32], for details about the REST endpoint). The GET returns:

```
{
  "adminState" : "disabled",
  "operState" : "init",
  "progressReport" : ""
}
```

This state is a transitory valid state while the sync process is starting up. Receiving a response with status code 422 and user message "External IdP synchronization is still initializing." is not necessarily an issue.

This is an issue if such condition persists even after all instances of `idmserv` are in `ONLINE` state, signaling that the Federated Identity Synchronization application is not able to establish a connection with the GIC application. This can happen because all `secserv` instances are not in `ONLINE` state. See the document ENM System Administrator Guide, Reference [1], for more details about how to check state of instances of a Service Group.

Recommendation or Workaround

If all `secserv` instances are not in `ONLINE` state, perform restart procedure for all `secserv` instances until at least one of them goes `ONLINE`. See the document ENM System Administrator Guide, Reference [1], for more details about how to restart instances of a Service Group.

14.2.4 Synchronization REST Failed with "httpStatusCode": 500, "userMessage":"EServiceNotFoundException", appName: ":generic-identity-config-service-ear"

Prerequisites

— User has mandatory roles: SECURITY_ADMIN.

— User executes command from UI or NBI.

Cause

The Federated Identity Synchronization application (running on `idmserv` service group) is not able to connect to a remote EJB service exposed by the GIC application (running on `secserv` service group). GIC provides access to PostgreSQL database containing the persistent configuration data of Federated Identity Synchronization application.

This could happen because all `secserv` instances are not in `ONLINE` state. See the document ENM System Administrator Guide, Reference [1], for more details about how to check state of instances of a Service Group.

Recommendation or Workaround

If all `secserv` instances are not in `ONLINE` state, perform restart procedure for all `secserv` instances until at least one of them goes `ONLINE`. See the document ENM System Administrator Guide, Reference [1], for more details about how to restart instances of a Service Group.

14.2.5 Synchronization REST Failed with "httpStatusCode": 422, "userMessage":"External IdP synchronization operation not allowed in current state."

Prerequisites

— User has mandatory roles: SECURITY_ADMIN.

— User executes command from UI or NBI.

Cause

The invoked REST is not allowed in the current Federated Identity Synchronization state. See the sections related to *Federated Identity Management* in the document ENM Identity and Access Management System Administrator Guide, Reference [20] for more information about the Federated Identity Synchronization state and use cases requirements.

Recommendation or Workaround

Set the Federated Identity Synchronization state to the desired state to perform the desired REST. See the section *Federated Identity Management Interface* in the document ENM System Security Configuration Programmers Guide, Reference [32] for details about the REST endpoints.

The following table shows the possible solution to failed use cases with status code 422 and user message `External IdP synchronization operation not allowed in current state.`

Table 14

Failed Used Case	REST	Solution or Action Required
IDAM-FIDMNBI05 NBI Update Federated Users Synchronize Period	PUT /oss/fidm/sync/period	— set sync admin state to disabled — update the sync period — set sync admin state to enabled (if wanted).
IDAM-FIDMNBI03 NBI Import Federated Users Synchronizer Advanced Settings	POST /oss/fidm/sync/import	— set sync admin state to disabled — import the sync advanced settings — set sync admin state to enabled (if wanted).
IDAM-FIDMNBI01 NBI Test Federated Users Synchronize Setting	POST /oss/fidm/sync/test	— set sync admin state to disabled — test the imported sync advanced settings — set sync admin state to enabled (if wanted).
IDAM-FIDMNBI09 NBI Delete Federated Users	POST /oss/fidm/sync/delete	— set sync admin state to disabled — delete all federated users from ENM Local IdP — set sync admin state to enabled (if wanted).
IDAM-FIDMNBI08 NBI Force Federated Users Synchronization	POST /oss/fidm/sync/forced	— set sync admin state to enabled — force the sync — set sync admin state to disabled (if wanted)
IDAM-FIDMNBI10 NBI Federated Users Synchronizer Restore to Default Advanced Settings	POST /oss/fidm/sync/restore	— set sync admin state to disabled — delete all federated users from ENM Local IdP — set sync admin state to enabled (if wanted).

14.2.6 Synchronization REST Failed with "httpStatusCode": 422, "userMessage":"External IdP synchronization is not yet configured."

Prerequisites

— User has mandatory roles: SECURITY_ADMIN.

— User executes command from UI or NBI.

Cause

The Federated Identity Synchronization Advanced Settings not yet configured in the system using the import option.

See the sections related to *Federated Identity Management* in the document ENM Identity and Access Management System Administrator Guide, Reference [20] for more information about the Federated Identity Synchronization.

This condition can be verified performing the get of the synchronization state (see the section *Get Federated Identity Synchronization State* in the document ENM System Security Configuration Programmers Guide, Reference [32], for details about the REST endpoint). The GET returns:

```
{
  "adminState" : "disabled",
  "operState" : "notConfigured",
  "progressReport" : ""
}
```

Recommendation or Workaround

Import the Federated Identity Synchronization Advanced Settings. See the section *Import Federated Identity Synchronization Advanced Settings* in the document ENM System Security Configuration Programmers Guide, Reference [32], for details about the REST endpoint.

14.2.7 Get Last Sync Report REST Failed with "httpStatusCode": 422, "userMessage":"External IdP synchronization never executed."

Prerequisites

— User has mandatory roles: SECURITY_ADMIN.

— User executes command from UI or NBI.

Cause

None of the synchronization actions (forcedSync, periodicSync, testSync, forcedDelete) has been ever performed in the system. This can happen also after

having performed a Restore To Defaults operation and until the first synchronization action finishes.

See the sections related to *Federated Identity Management* in the document ENM Identity and Access Management System Administrator Guide, Reference [20] for more information about the Federated Identity Synchronization.

Recommendation or Workaround

Perform at least one synchronization action (forcedSync, periodicSync, testSync, forcedDelete). When the action finishes, the last sync report is available. See the section *Federated Identity Management Interface* in the document ENM System Security Configuration Programmers Guide, Reference [32], for details about the REST endpoint.

14.2.8 Get Last Sync Report REST Returns Failed Action

The Federated Identity Synchronization manages the following asynchronous operations (actions):

- Periodic Sync
- Forced Sync
- Test Sync
- Forced Delete

Any action is subdivided in steps (task):

Table 15

State	Description
externalSearch	Searching from External IdP.
internalSearch	Searching from Local IdP (OpenDJ).
merge	Merging results between Internal and External Federated users.
performCrud	Performing CRUD operations on Local IdP (OpenDJ) and verifying their results.

The sequence of tasks depends on the involved action.

For Periodic and Force Sync actions, the sequence of tasks is:

1. externallySearching
2. internallySearching
3. merging
4. performingCrud

For Test Sync action, the sequence of tasks is:

1. externallySearching
2. internallySearching
3. merging

For Forced Delete action, the sequence of tasks is:

1. internallySearching
2. merging
3. performingCrud (Delete ONLY)

Prerequisites

— User has mandatory roles: SECURITY_ADMIN.

— User executes command from UI or NBI or a Periodic Sync is automatically triggered by Federated Identity Synchronization application.

Cause

A failed action (field "result" equal to "failed" in "actionReport" section of the Last Sync Report) is generally caused by LDAP errors during either the externalSearch or the internalSearch task.

Any LDAP errors prevent from completing the action and the steps subsequent the failed one are skipped. The failed task can be determined by analyzing the Last Sync Report (it is the first entry in the "taskReports" list with field "result" equal to "failed").

Recommendation or Workaround

The possible workaround depends on the failed task and on the value and diagnosticMessages of the reported error counters.

Table 16

Failed Task	Counter	Value	DiagnosticMessages	Solution or Action Required
externalSearch	numBindRequestsError	greater than 0	["Operations Error"]	— The Primary and Secondary Server addresses used to access External IdP can be wrong (wrong IP address and/or port). See the section *LDAP*

Failed Task	Counter	Value	DiagnosticMessages	Solution or Action Required
				Connection Setup in the document ENM Identity and Access Management System Administrator Guide, Reference [20], for more details. — The LDAP Connection Mode used to access External IdP is configured as Secure (LDAPS) but the External CA has not been correctly added to ENM trustors (see the section *Update Trust Profile IdP_NBI_TP with an External CA Already Imported in PKI* in the document ENM Identity and Access Management System Administrator Guide, Reference [20], for more details).
externalSearch	numBindRequestsError	greater than 0	["Invalid Credentials"]	The Proxy Account Distinguish Name and/or the Proxy Account Password used to access External IdP can be wrong. See the section *LDAP Connection Setup* in the document ENM Identity and Access Management System Administrator Guide, Reference [20], for more details.
externalSearch	numSearchRequestsError	greater than 0	["No Such Entry"]	— The Base Distinguish Name used to access External IdP can be wrong. See the section *LDAP Connection Setup* in the document ENM Identity and Access Management System Administrator Guide, Reference [20], for more details.

Failed Task	Counter	Value	DiagnosticMessages	Solution or Action Required
				— The relative base DN specified in the imported Federated Identity Synchronization Advanced Settings can be wrong (see the section *Federated Identity Synchronization Advanced Settings* in the document ENM Identity and Access Management System Administrator Guide, Reference [20], for more details). Import the Federated Identity Synchronization Advanced Settings specifying the correct search relative base DN. See the section *Import Federated Identity Synchronization Advanced Settings* in the document ENM System Security Configuration Programmers Guide, Reference [32], for details about the REST endpoint.
externalSearch	numSearchRequestsError	greater than 0	["Size Limit Exceeded"]	The search page size specified in the imported Federated Identity Synchronization Advanced Settings is greater than or equal to the size limit defined in the External IdP. Import the Federated Identity Synchronization Advanced Settings specifying a search page size less than the size limit defined in the External IdP. See the section *Import Federated Identity Synchronization Advanced Settings* in the document ENM System Security Configuration Programmers Guide, Reference [32], for details about the REST endpoint.

Failed Task	Counter	Value	DiagnosticMessages	Solution or Action Required
externalSearch	numSearchRequestsError	greater than 0	["Insufficient Access Rights"]	The Proxy Account used to access External IdP cannot have the unindexed search privilege assigned on the External IdP. See the section *External Identity Provider Prerequisites* in the document ENM Identity and Access Management System Administrator Guide, Reference [20], for more details.
internalSearch	numSearchRequestsError	greater than 0	["Insufficient Access Rights"]	The internal authenticated user used to access Local IdP (OpenDJ) cannot have the unindexed search privilege in OpenDJ. See the section *Unindexed Search* in the document ENM Identity and Access Management System Administrator Guide, Reference [20], for more details about how to assign the required privilege.

14.2.9 Get Last Sync Report REST Returns performCrud Task Report with numUserCreateErrorDueToInternalLogicException Counter

Prerequisites

— User has mandatory roles: SECURITY_ADMIN.

— User executes command from UI or NBI or a Periodic Sync is automatically triggered by Federated Identity Synchronization application.

Cause

Federated Identity Synchronization is not able to create federated users because users with same username are already present in ENM. This can happen, for example, if same users had been already created in ENM as Remote user according to the Authentication with External Identity Provider feature. The details about which federated users cannot be created can be found in Log Viewer (see the section *Federated Identity Synchronization and Log Viewer* in the document ENM Identity and Access Management System Administrator Guide, Reference [20] for more details).

Recommendation or Workaround

Check in **ENM GUI-User Management** the actual presence of users created in ENM (as Local or Remote) and evaluate if they must be removed before running again a federated identity synchronization.

14.2.10 Get Last Sync Report REST Returns performCrud Task Report with numUserCreateErrorDueToEntityNotFound Counter

Prerequisites

— User has mandatory roles: SECURITY_ADMIN.

— User executes command from UI or NBI or a Periodic Sync is automatically triggered by Federated Identity Synchronization application.

Cause

Federated Identity Synchronization is not able to create federated users because required roles and target groups have not been preliminary created in ENM (see the section *ENM Prerequisites* in the document ENM Identity and Access Management System Administrator Guide, Reference [20], for more details).

The details about which federated users with which role or target groups cannot be created can be found in Log Viewer (see the section *Federated Identity Synchronization and Log Viewer* in the document ENM Identity and Access Management System Administrator Guide, Reference [20], for more details).

Recommendation or Workaround

Check in **ENM GUI-Role Management** and **Target Group Management** the actual presence of required custom roles and target groups and possibly create the missing ones before running again a federated identity synchronization.

14.2.11 Get Last Sync Report REST Returns performCrud Task Report with numUserUpdateErrorDueToEntityNotFound Counter

Prerequisites

— User has mandatory roles: SECURITY_ADMIN.

— User executes command from UI or NBI or a Periodic Sync is automatically triggered by Federated Identity Synchronization application.

Cause

Federated Identity Synchronization is not able to update federated users because required roles and target groups have not been preliminary created in ENM (see the section *ENM Prerequisites* in the document ENM Identity and Access Management System Administrator Guide, Reference [20], for more details).

The details about which federated users with which role or target groups cannot be updated can be found in Log Viewer (see the section *Federated Identity Synchronization and Log Viewer* in the document ENM Identity and Access Management System Administrator Guide, Reference [20], for more details).

Since an update is triggered, the user was successfully created with required roles or target groups correctly configured in ENM, but likely new roles and target groups were added in external IdP without creating the correspondent ones in ENM.

Recommendation or Workaround

Check **ENM GUI-Role Management** and **Target Group Management** the actual presence of required custom roles and target groups and possibly create the missing ones before running again a federated identity synchronization.

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