

Update NeLS Connection

Virtual Multimedia Resource Function

Operating Instructions

Copyright

© Ericsson AB 2017–2019. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

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	Introduction	1
2	Configure SSL Connection	2
2.1	Enable the Customer Security Layer	2
2.2	Disable the Customer Security Layer	3
2.3	Update SSL Certificates	4
3	Configure the NeLS Connection	6





1 Introduction

This document describes how to update the NeLS connection.

Communication between LM and NeLS requires Secure Sockets Layer (SSL). This network connection can be secured by two layers of encryption, as follows:

- Ericsson security layer
- Customer security layer

The NeLS connection is always encrypted using SSL certificates provided by Ericsson. Optionally, a second security layer, using the network operator's SSL certificates, is available.



2 Configure SSL Connection

2.1 Enable the Customer Security Layer

The optional customer encryption layer between LM and NeLS requires the network SSL certificates of the operator and updates to the `/storage/system/config/lm-apr9010503/certs/certificate_config.xml` file.

Steps

1. From a terminal window, use `ssh` to connect to the System Controller (SC) where LM is active.

Note: To identify the SC where LM is active, execute the following command from any SC: `cmw-status -v siass | grep -A 1 LmSa`.

`safSISU=safSu=LmSa-Su-0\, HASstate=ACTIVE(1)` indicates that LM is active in SC-1.

2. Store the following SSL files in `/storage/system/config/lm-apr9010503/certs`:

Note: The following files are unique to your network environment:

- The Certificate Authority (CA) file
- The Client Certificate file
- The Client Private Key file

3. Update `/storage/system/config/lm-apr9010503/certs/certificate_config.xml` with the SSL configuration file names.

Example

The following example shows the structure of `certificate_config.xml`:

```
<?xml version="1.0" encoding="utf-8"?>
<nels-ssl-config>
  <certificate-authority>
    <path>certificate-authority-file-name</path>
  </certificate-authority>
  <client-certificate>
    <path>client-certificate-file-name</path>
  </client-certificate>
  <client-private-key>
    <path>client-private-key-file-name</path>
  </client-private-key>
</nels-ssl-config>
```



```
</client-private-key>
</nels-ssl-config>
```

- Note:**
- *<certificate-authority>* is the certificate authority file name. The file must contain all certificates in the certificate chain.
 - *<client-certificate>* is the client certificate file name.
 - *<client-private-key>* is the client private key file name.

30 seconds after changing any files in `/storage/system/config/lm-apr9010503/certs` from the SC where LM is active, LM attempts to connect to NeLS using the SSL configuration settings stored in `certificate_config.xml`.

4. If required, configure the `NeLSConfiguration.host` and `NeLSConfiguration.port` attributes in the LM MOM. For more information, see [Configure the NeLS Connection](#) on page 6.

After This Task

After configuring the customer security layer, it is highly recommended to perform a system backup with the Backup and Restore Framework (BRF) to preserve the certificate files.

2.2 Disable the Customer Security Layer

When the optional customer security layer is disabled, all configuration values must be removed from `/storage/system/config/lm-apr9010503/certs/certificate_config.xml`.

Steps

1. From a terminal window, use `ssh` to connect to the System Controller (SC) where LM is active.

Note: To identify the SC where LM is active, execute the following command from any SC: `cmw-status -v siass | grep -A 1 LmSa`.

`safSISU=safSu=LmSa-Su-0\, . . . HASstate=ACTIVE(1)` indicates that LM is active in SC-1.

2. Verify that `/storage/system/config/lm-apr9010503/certs/certificate_config.xml` has empty values for all SSL file names.

Example

The following example shows the structure of `certificate_config.xml` when the customer security layer is properly disabled:



```
<?xml version="1.0" encoding="utf-8"?>
  <nels-ssl-config>
    <certificate-authority>
      <path></path>
    </certificate-authority>
    <client-certificate>
      <path></path>
    </client-certificate>
    <client-private-key>
      <path></path>
    </client-private-key>
  </nels-ssl-config>
```

3. If required, update `certificate_config.xml` to remove the file names.

30 seconds after updating `certificate_config.xml`, LM automatically reloads the SSL configuration settings and attempts to reestablish communication with NeLS using only the Ericsson security layer.

2.3 Update SSL Certificates

The SSL certificate files used by the customer security layer are unique to your network environment and can be updated as required.

Steps

1. From a terminal window, use `ssh` to connect to the System Controller (SC) where LM is active.

Note: To identify the SC where LM is active, execute the following command from any SC: `cmw-status -v siass | grep -A 1 LmSa`.

`safSISU=safSu=LmSa-Su-0\, . . . HASState=ACTIVE(1)` indicates that LM is active in SC-1.

2. If required, transfer all updated certificate files to the SC.
3. Copy the updated certificate files to `/storage/system/config/lm-apr9010503/certs`, using the following command for each file:

```
cp <storage location>/<SSL certificate file> /storage/system/
config/lm-apr9010503/certs/<SSL certificate file>
```

Note: If multiple Certificate Authorities are required, all CAs must be defined in a single CA file. At least one CA must be valid for a successful NeLS connection.

4. If required, update `/storage/system/config/lm-apr9010503/certs/certificate_config.xml` with the new SSL configuration file names.



If LM is connected to NeLS, changes made to `/storage/system/config/lm-apr9010503/certs` from the SC where LM is active cause the NeLS connection to drop after 30 seconds. After dropping the connection, LM automatically reloads the SSL configuration from `certificate_config.xml` and attempts to reestablish the NeLS connection.

After reloading the SSL configuration, the updated certificate files are in use.

5. Wait 30 seconds, then open the COM CLI, using the following command:

```
/opt/com/bin/cliss
```

6. Check connectivity by printing the NeLS connection status:

```
show  
ManagedElement=1, SystemFunctions=1, Lm=1, NeLSConfiguration=1,  
connectionStatus
```

Note:

`connectionStatus=CONNECTED` indicates that the SSL configuration update was successful and a connection to NeLS has been reestablished.

While LM is operating in Normal mode, any problem with the SSL certificate files or `certificate_config.xml` prevents LM from reestablishing communication with NeLS and triggers a transition to Autonomous mode. For more information on resolving SSL certificate issues, refer to [License Management, Autonomous Mode Activated](#).

After This Task

After successfully updating the customer security layer, it is highly recommended to perform a system backup with BRF to preserve the new certificate files.



3 Configure the NeLS Connection

LM must be configured to direct license requests to NeLS using the `NeLSConfiguration.host` and `NeLSConfiguration.port` attributes in the LM MOM.

Steps

1. From a terminal window, use `ssh` to connect to the COM CLI Management System server port where the active COM CLI is running:

```
ssh <username>@<blade_IP_address> -p 22 -t -s cli
```

Note: The default COM CLI Management System server port is 22.

2. Verify that the NeLS configuration points to the correct network location and port by issuing the following commands:

```
show verbose
ManagedElement=1, SystemFunctions=1, Lm=1, NeLSConfiguration=1,
host
```

```
show verbose
ManagedElement=1, SystemFunctions=1, Lm=1, NeLSConfiguration=1,
port
```

3. If required, update the NeLS configuration by executing the following commands in the COM CLI:

```
configure

ManagedElement=1, SystemFunctions=1, Lm=1, NeLSConfiguration=1

host=<IP_Address_or_FQDN>
port=<Port_Number>
commit
```

The connection to NeLS has been configured. After committing the configuration changes, LM drops the current NeLS connection, if one is established, and attempts to reconnect using the updated configuration settings.

4. After verifying the configuration, check connectivity by printing the NeLS connection status, using the following command:

```
show
ManagedElement=1, SystemFunctions=1, Lm=1, NeLSConfiguration=1,
connectionStatus
```

**Note:**

`connectionStatus=CONNECTED` indicates that a connection to NeLS is established.

5. Retrieve license information from the NeLS and publish it to the information model using the following MO action:

`ManagedElement=1, SystemFunctions=1, Lm=1, publishLicenseInventory`

6. Exit the COM CLI:

`exit`