

Configure SSL Connection to NeLS

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2017. 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	Description	1
2	Procedure	1
2.1	Correct Issues When the Customer Security Layer is Disabled	2
2.2	Correct Issues with the Customer Security Layer	4





1 Description

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

- Ericsson security layer
- Customer security layer

The NeLS connection must always be encrypted using SSL certificates provided by Ericsson. The customer security layer, using the SSL certificates of the operator, must be enabled only if NeLS is configured with network operator node credentials. A faulty SSL setup can lead to connectivity issues.

2 Procedure

Prerequisites

- No documents are required.
- No tools are required.
- The following conditions must apply:
 - No ongoing maintenance activities are affecting the network or Network Elements.
 - The host address and port number of the NeLS server is known.
 - The ME has a working connection to NeLS.
 - If an operator tunnel is used for the connection to NeLS, the corresponding certificate is available.
 - The user has Linux[®] shell access to the System Controllers (SCs).
 - An Ericsson Command-Line Interface (ECLI) session in Exec mode is in progress.



2.1 Correct Issues When the Customer Security Layer is Disabled

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

Steps

1. Identify the SC where LM is active by executing the following command from any SC:

```
cmw-status -v siass | grep -A 1 lm
```

Note: On legacy installations, use the command `cmw-status -v siass | grep -A 1 LmSa` instead.

The following is an example output where LM is active on SC-1:

```
safSISU=safSu=SC-1\,safSg=2N\,...  
    HState=ACTIVE(1)  
--  
safSISU=safSu=SC-2\,safSg=2N\,...  
    HState=STANDBY(2)
```

The following is an example output where LM is active on SC-2:

```
safSISU=safSu=SC-1\,safSg=2N\,...  
    HState=STANDBY(1)  
--  
safSISU=safSu=SC-2\,safSg=2N\,...  
    HState=ACTIVE(2)
```

Note: On legacy installations, SC-1 and SC-2 in the output is indicated with `safSISU=safSu=LmSa-Su-0` and `Su-1`, respectively.

2. Use SSH to log on to the SC where LM is active, for example:

```
ssh <user>@<hostname> -p 7022
```

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

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>
```

Note: If `certificate_config.xml` is missing, recreate it from the original template:

```
cp /opt/lm/etc/certificate_config_template.xml ⇒
/storage/system/config/lm-apr9010503/certs/certificate_config.xml
```

4. If necessary, update `certificate_config.xml` by removing the filenames within the `<path></path>` tags.

Wait 30 seconds after updating `certificate_config.xml`; LM automatically reloads the SSL configuration settings and attempts to reestablish communication with NeLS.

5. In the ECLI, check the status of the connection to NeLS in the *NeLSConfiguration* Managed Object (MO), for example:

```
>show ManagedElement=NODE06ST,SystemFunctions=1,Lm=1,NeLSConfiguration=1,connectionStatus
```

The following is an example output:

```
connectionStatus=CONNECTED
```

6. If the NeLS and SSL configurations are valid but `connectionStatus=NOT_CONNECTED`, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

Note: If resolving the issue is expected to take more than 24 hours, Emergency Unlock can be used to prevent the system from entering Locked Mode. For more information on Emergency Unlock, refer to the *Activate Emergency Unlock Mode*.

After successfully configuring the SSL connection, it is highly recommended to perform a system backup with the Backup and Restore Framework (BRF).



2.2 Correct Issues with the Customer Security Layer

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

Steps

1. Identify the SC where LM is active by executing the following command from any SC:

```
cmw-status -v siass | grep -A 1 lm
```

Note: On legacy installations, use the command `cmw-status -v siass | grep -A 1 LmSa` instead.

The following is an example output where LM is active on SC-1:

```
safSISU=safSu=SC-1\,safSg=2N\,...  
    HASState=ACTIVE(1)  
--  
safSISU=safSu=SC-2\,safSg=2N\,...  
    HASState=STANDBY(2)
```

The following is an example output where LM is active on SC-2:

```
safSISU=safSu=SC-1\,safSg=2N\,...  
    HASState=STANDBY(1)  
--  
safSISU=safSu=SC-2\,safSg=2N\,...  
    HASState=ACTIVE(2)
```

Note: On legacy installations, SC-1 and SC-2 in the output is indicated with `safSISU=safSu=LmSa-Su-0` and `Su-1`, respectively.

2. Use SSH to log on to the SC where LM is active, for example:

```
ssh <user>@<hostname> -p 7022
```

3. Ensure that the following SSL files are located in `/storage/system/config/lm-apr9010503/certs/`:

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

If any of these files are missing, or if new files are required, follow the internal processes of the operator to obtain replacements and store them in `/storage/system/config/lm-apr9010503/certs/`.



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. Verify that `certificate_config.xml` in `/storage/system/config/lm-apr9010503/certs/` references the correct SSL filenames.

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-filename</path>
  </certificate-authority>
  <client-certificate>
    <path>client-certificate-filename</path>
  </client-certificate>
  <client-private-key>
    <path>client-private-key-filename</path>
  </client-private-key>
</nels-ssl-config>
```

Where:

`certificate-authority-filename` is the certificate authority filename. The file must contain all certificates in the certificate chain.

`client-certificate-filename` is the client certificate filename.

`client-private-key-filename` is the client private key filename.

Note: If `certificate_config.xml` is missing, recreate it from the original template:

```
cp /opt/lm/etc/certificate_config_template.xml =>
/storage/system/config/lm-apr9010503/certs/certificate_config.xml
```

5. If necessary, update `certificate_config.xml` with the correct filenames in the `<path></path>` tags.

Wait 30 seconds after updating `certificate_config.xml`; LM automatically reloads the SSL configuration settings and attempts to reestablish communication with NeLS.

6. In ECLI, check the status of the connection to NeLS in the *NeLSConfiguration* MO, for example:

```
>show ManagedElement=NODE06ST, SystemFunctions=1, Lm=1, NeLSConfiguration=1, connectionStatus
```

The following is an example output:



```
connectionStatus=CONNECTED
```

7. If the NeLS and SSL configurations are valid but `connectionStatus=NOT_CONNECTED`, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

Note: If resolving the issue is expected to take more than 24 hours, Emergency Unlock can be used to prevent the system from entering Locked Mode. For more information on Emergency Unlock, refer to the *Activate Emergency Unlock Mode*.

After successfully configuring the SSL connection, it is highly recommended to perform a system backup with BRF to preserve the certificate files.