

License Management, Key File Fault

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

2	Alarm Description	2
3	Prerequisites	4
3.1	Documents	4
3.2	Tools	4
3.3	Conditions	4
4	Procedure	5
4.1	Correct NeLS Configuration Issues	5
4.2	SSL Certificate Issues	8







2 Alarm Description

The License Management, Key File Fault alarm is raised when the License Manager (LM) transitions to Locked mode. This is a critical situation that may prevent the Managed Element from using licensed features and functionality.

Locked mode is initiated at the end of the 24 hour Autonomous mode period if the Network License Server (NeLS) is unreachable.

The possible alarm causes and fault locations are explained in [Table 1](#).

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
159	License Management, Key File Fault	NeLS is unreachable	NeLS server	No license handling
			Possible IP network issue	
			Domain Name System (DNS) server	
			Network interface	

Note: The alarm can be raised as a result of maintenance activities.

During Locked mode, requests for licensed features and capacities are blocked by LM.

The alarm attributes are listed and explained in [Table 2](#).

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	393221
Managed Object Class	Lm
Managed Object Instance	ManagedElement=<node_name>, SystemFunctions=1, Lm=1
Specific Problem	License Management, Key File Fault
Event Type	qualityOfServiceAlarm (3)



Attribute Name	Attribute Value
Probable Cause	configurationOrCustomisationError (159)
Additional Text	Key file fault in Managed Element
Perceived Severity	critical (3)



3 Prerequisites

This section provides information on the documents, tools, and conditions that apply to the procedure.

3.1 Documents

This instruction references the following documents:

- Activate Emergency Unlock Mode
- Data Collection Guideline for vMRF

3.2 Tools

No tools are required.

3.3 Conditions

Before starting this procedure, ensure that the following conditions are met:

- A License Management, Key File Fault alarm is raised.
- No ongoing maintenance activities are affecting the network or network elements.
- The host address and port number of NeLS is available.
- Have access to the network operator's Secure Sockets Layer (SSL) certificates for the optional NeLS customer security layer.
- The user has proper authority to handle configuration management of the network elements.
- Linux® shell access to the System Controllers (SCs).
- Access to an Ericsson Command-Line Interface (ECLI).



4 Procedure

The following procedure describes how to cease a License Management, Key File Fault alarm.

4.1 Correct NeLS Configuration Issues

The NeLS server address and port number are configured using `NeLSConfiguration.host` and `NeLSConfiguration.port` attributes. A faulty configuration can lead to connectivity issues.

Steps

1. Ensure that the network infrastructure (physical connections, firewalls, routers, and so on) allows communication between LM and NeLS.
2. 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.

3. Check the NeLS connection status:

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

The command returns with one of the following printouts:

- `connectionStatus=UNDEFINED` indicates that LM has not made an initial connection attempt to NeLS.
- `connectionStatus=CONNECTED` indicates that a connection to NeLS is established.
- `connectionStatus=NOT_CONNECTED` indicates that the NeLS connection is down.
- If the connection status is `CONNECTED`, check the alarm status.

If the alarm is still active, consult the next level of maintenance support. Further actions are outside the scope of this instruction.



Note: Emergency Unlock can be used to temporarily restore access to licensed functionality while the system is in locked mode. For more information on Emergency Unlock, see [License Management](#).

- If the `connectionStatus` is `UNDEFINED` or `NOT_CONNECTED`, verify that the `NeLSConfiguration` points to the correct host address and port number:

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

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

4. 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 attempts to reconnect using the updated configuration settings.

5. Check the NeLS connection status:

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

- If `connectionStatus=CONNECTED`, the NeLS connection has been restored.
- If `connectionStatus=NOT_CONNECTED`, continue with the next step.

6. Use the `Telnet` command to attempt to reach NeLS from the SC VM where LM is running.

```
telnet <NeLS_IP_Address:Port>
```

The following output shows that the NeLS is down:

```
Trying <NeLS_IP_Address>...  
telnet: connect to address <IP_Address>: No route to host
```



- If the NeLS is down, wait five minutes and retry the command. If the output is the same, consult the next level of maintenance support. Further actions are outside the scope of this instruction.
 - If the NeLS is reachable, continue with the next step.
7. Check the NeLS connection retry interval through the COM CLI, and take note of the setting:

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

8. Wait for the retry interval to elapse. If required, update the attribute to a shorter interval with the following commands:

```
configure  
  
ManagedElement=1, SystemFunctions=1, Lm=1, NeLSConfiguration=1  
retryInterval=<new_retry_interval_in_seconds>  
  
commit
```

9. After the retry interval and a short grace period have elapsed, check the connection status:

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

Note: If `retryInterval` was modified, the change may need to be reverted. To reset the `retryInterval`, execute the following command:

```
configure ManagedElement=1, SystemFunctions=1, Lm=1,  
NeLSConfiguration=1 retryInterval=commit
```

10. If the connection status is `CONNECTED`, check the alarm status.

If the alarm is still active, consult the next level of maintenance support. Further actions are outside the scope of this instruction.

Note: Emergency Unlock can be used to temporarily restore access to licensed functionality while the system is in locked mode. For more information on Emergency Unlock, see [License Management](#).

11. If the connection status is `NOT_CONNECTED`, investigate possible certificate issues by following the steps in [SSL Certificate Issues](#) on page 8.



4.2 SSL Certificate Issues

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. Optionally, a second security layer, using the SSL certificates of the network operator, is available. A faulty SSL setup can lead to connectivity issues.

4.2.1 Correct Issues When the Customer Security Layer is Disabled

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) VM 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.

4. If `certificate_config.xml` is missing, recreate it from the original template with the following command:

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

After recreating the file, update it as required.

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

5. If the NeLS and SSL configurations are valid and `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, see [License Management](#).

After This Task

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

4.2.2

Correct Issues with 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) VM where LM is active.

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



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

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

If any of these files are missing, or if new files are required, follow your internal processes 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.

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 `/storage/system/config/lm-apr9010503/certs/certificate_config.xml`.

3. Verify that `certificate_config.xml` references the correct SSL 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>
```

- 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.

4. 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.

5. 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
```

After recreating the file, update it as required.

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

6. If the NeLS and SSL configurations are valid and `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, see [License Management](#).

After This Task

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