

License Management, Key File Fault

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	Alarm Description	1
2	Procedure	1
2.1	Handle Alarm License Management, Key File Fault	1





1 Alarm Description

The alarm is raised when license information is unreachable in NeLS for more than 24 hours.

Table 1 License Management, Key File Fault Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
Failing to reach license information in NeLS for more than 24 hours	The license information remains unreachable for the Managed Element (ME) after the configured Autonomous mode period (usually 24 hours). The ME enters Locked mode	NeLS is unreachable or the relevant License Key File is corrupted or missing.	NeLS server	Service is limited to the features and capacity granted to the ME that are already reserved and continue to function normally, until cluster restart.
			TLS configuration in ME	
			Possible IP network issue	
			Domain Name System (DNS) server	
			Network interface	

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

2 Procedure

2.1 Handle Alarm License Management, Key File Fault

Prerequisites

- This instruction references the following documents:
 - *Activate Emergency Unlock Mode*
 - *Data Collection Guideline*
- No tools are required.
- The following conditions must apply:
 - The alarm is raised.



- No ongoing maintenance activities are affecting the network or network elements.
- The host address and port number of the NeLS server is known.
- Transport Layer Security to NeLS with one or two tunnels is set up with the relevant certificates.
- The user has Linux[®] shell access to the System Controllers (SCs).
- An Ericsson Command-Line Interface (ECLI) running in exec mode.

Steps

1. If there are any network-related alarms on the ME, act on them first.
2. In the ECLI, check the connection status 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=NOT_CONNECTED
```

3. Select action according to the `connectionStatus` attribute value:

- If `UNDEFINED` or `NOT_CONNECTED`, proceed with Step 5.
- If `CONNECTED`, continue with the next step.

4. Check the alarm status. Is the alarm still active?

No: Proceed with Step 16.

Yes: Continue with the next step.

5. Verify that the `NeLSConfiguration` attributes of the *NeLSConfiguration* MO point to the correct host address and port number:

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

```
host=<IP_Address_or_FQDN>
```

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

```
port=<Port_Number>
```

6. If necessary, update the connection parameters to NeLS:

```
>configure
```



```
(config)>ManagedElement=NODE06ST, SystemFunctions=1, Lm=1, NeLSConfiguration=1
```

```
(config-NeLSConfiguration=1)>host=<IP_Address_or_FQDN>
```

```
(config-NeLSConfiguration=1)>port=<Port_Number>
```

```
(config-NeLSConfiguration=1)>commit
```

After committing the configuration changes, LM attempts to reconnect using the updated connection settings.

7. Check the connection status to NeLS:

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

The following is an example output:

```
connectionStatus=CONNECTED
```

8. Is the `connectionStatus` attribute value `CONNECTED`?

Yes: Proceed with Step 13.

No: Continue with the next step.

9. From a Linux shell on the SC of the ME, use `ping` and `traceroute` to attempt to reach the NeLS host address.

If NeLS is unreachable, wait five minutes and retry the command. If the result is still the same, proceed with Step 14.

10. If NeLS was reachable, check the NeLS connection retry interval using the ECLI:

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

The following is an example output:

```
retryInterval=30
```

Write down or memorize the current setting.

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

```
>configure
```

```
(config)>ManagedElement=NODE06ST, SystemFunctions=1, Lm=1, NeLSConfiguration=1
```



```
(config-NeLSConfiguration=1) >retryInterval=<seconds>
```

```
(config-NeLSConfiguration=1) >commit
```

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

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

The following is an example output:

```
connectionStatus=CONNECTED
```

Note: If `retryInterval` was modified, revert the change to the original value using the commands in Step 11.

13. Check the alarm status. Is the alarm still active?

Yes: Continue with the next step.

No: Proceed with Step 16.

14. Perform data collection, refer to *Data Collection Guideline*.

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

15. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.
16. Job is completed.