

LOTC Time Synchronization

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2014–2017. 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 | 2 |
| 2.1 | Handle Alarm LOTC Time Synchronization | 2 |
| 2.2 | Handle Reason Time Difference over Threshold | 3 |
| 2.3 | Handle Reason Unusable Time Servers | 3 |
| 2.4 | Handle Reason Rejected Time Servers | 4 |
| 2.5 | Handle Reason Unreachable Time Servers | 4 |





1 Alarm Description

The alarm is raised in the following situations:

- The time difference within the cluster exceeds tolerance.
- The Managed Element (ME) fails to use the Network Time Protocol (NTP) service.

Table 1 LOTC Time Synchronization Alarm Causes

| Alarm Cause | Description | Fault Reason | Fault Location | Impact |
|--|---|--|--|--|
| Time difference within the cluster exceeds tolerance | There are time differences between the hosts in the cluster exceeding the threshold value of 10 seconds | Timing within the cluster is disrupted because of maintenance activities | One or more hosts can be rebooting | Time stamps used in cluster services (such as logging, alarms, or charging records) start to differ from the real time |
| | | A host is rebooting | | |
| Failing to use the NTP service | The configured NTP servers do not respond to a request for time synchronization or provide an invalid answer to the ME. The ME cannot use the NTP service. | One or more NTP servers are down (unreachable NTP servers) | NTP server | If one or more NTP servers are unreachable, the result is a loss in resilience with no service impact. If all NTP servers are unreachable, then time stamps used in cluster services (such as logging, alarms, or charging records) start to differ from the real time. |
| | | The ME rejected the time offered by the NTP server | NTP server configuration, firewall configuration | |
| | | Loss of connectivity to one or more NTP servers (unreachable NTP server) | Network problems | |
| | | The NTP server is unusable and its Fully Qualified Domain Name (FQDN) cannot be resolved | Domain Name System (DNS) server | |
| | | Faulty network interface | Network interface | |



Note: This alarm can appear as a result of a maintenance activity.

2 Procedure

2.1 Handle Alarm LOTG Time Synchronization

Prerequisites

- This instruction references the following document:
 - *Data Collection Guideline*
- No tools are required.
- The following conditions must apply:
 - The alarm is raised.
 - It is known how to map the `HostName` (part of alarm attribute `Source`) to its IP address.
 - The user has administrative privileges.

Steps

1. Check the `Additional Text` attribute of the alarm.
2. Select the appropriate action based on the attribute value:
 - If `Additional Text` contains `Time incorrect`, proceed with Section 2.2 Handle Reason Time Difference over Threshold on page 3.
 - If `Additional Text` contains `unusable`, proceed with Section 2.3 Handle Reason Unusable Time Servers on page 3.
 - If `Additional Text` contains `rejected`, proceed with Section 2.4 Handle Reason Rejected Time Servers on page 4.
 - If `Additional Text` contains `unreachable`, proceed with Section 2.5 Handle Reason Unreachable Time Servers on page 4.
 - For other cases, proceed with the next step.
3. Perform data collection, refer to *Data Collection Guideline*.
4. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.



2.2 Handle Reason Time Difference over Threshold

Steps

1. Log on to the host to access a Linux® shell, for example:

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

The hostname is part of alarm attribute *Source*.

2. Wait up to 20 minutes until the cluster reaches a stable state (that is, no node is rebooting). Check the state:

```
>cmw-status node
```

The following is an example output:

```
Status OK
```

3. Is the alarm cleared?

Yes: Proceed with Step 6.

No: Continue with the next step.

4. Perform data collection, refer to *Data Collection Guideline*.
5. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.
6. Job is completed.

2.3 Handle Reason Unusable Time Servers

Steps

1. Log on to the host to access a Linux shell, for example:

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

The hostname is part of alarm attribute *Source*.

2. Perform a lookup of the NTP server:

```
>nslookup <ntp_fqdn>
```

Note: The NTP server FQDN is pointed at by alarm attribute *Additional Text*.

3. Does the command return an error?

Yes: The DNS server can have a configuration fault. Request the DNS server administrator to act on the fault. Proceed with Step 6.



No: Continue with the next step.

4. Perform data collection, refer to *Data Collection Guideline*.
5. Consult the next level of maintenance support. Further actions are outside the scope of this instruction.
6. Job is completed.

2.4 Handle Reason Rejected Time Servers

Steps

1. Log on to the host to access a Linux shell, for example:

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

The hostname is part of alarm attribute `Source`.

2. Check the NTP status:

```
>ntpq -p
```

The NTP is functional if the output includes an active server, indicated by *. Backup sources are indicated with + in the output.

The following is an example output:

```
node1-kvml:~ # ntpq -p
remote refid st t when poll reach delay offset jitter
=====
+ns1.ericsson.se 192.0.2.10 2 u 239 1024 377 1.390 1.099 0.147
*ns2.ericsson.se 192.0.2.11 2 u 287 1024 377 1.260 1.272 0.181
+node2-kvml 193.180.251.38 3 u 735 1024 377 0.321 0.121 0.142
```

3. Does the output show that an NTP server is active?

Yes: The NTP server can have a configuration fault. Request the NTP server administrator to act on the fault. Proceed with Step 5.

No: Continue with the next step.

4. The network blocking the NTP traffic can have a configuration fault. Request the network administrator to act on the fault. Continue with the next step.
5. Job is completed.

2.5 Handle Reason Unreachable Time Servers

Steps

1. Log on to the host to access a Linux shell, for example:

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




The hostname is part of alarm attribute `Source`.

2. Is the affected node a payload node?

Yes: Proceed with Step 11.

No: Continue with the next step.

3. Check the connection to the NTP server using `ping` and `traceroute`.

The NTP server FQDN is pointed at by alarm attribute `Additional Text`.

4. Can the NTP server be reached with a delay less than 10 seconds?

Yes: Proceed with Step 6.

No: Continue with the next step.

5. The network can have a configuration fault. Request the NTP server administrator or network administrator to act on the fault. Proceed with Step 17.

6. Check the NTP configuration in configuration file `cluster.conf`.

7. Is the NTP server FQDN or IP address correct?

Yes: Proceed with Step 11.

No: Continue with the next step.

8. Update the NTP server FQDN or IP address in configuration file `cluster.conf`.

9. Validate the configuration:

```
>lde-config -v
```

10. Reload the updated configuration:

```
>lde-config --reload
```

11. Restart the alarm service:

```
>service lde-alarmd restart
```

12. Wait up to 20 minutes and check if the alarm is cleared. Is the alarm cleared?

Yes: Proceed with Step 17.

No: Continue with the next step.

13. Reboot the node.



Attention!

Risk of system malfunction or traffic disturbance.

As a consequence of a reboot, applications can lose sessions or traffic. Therefore, restart only one node at a time and only if the state of the cluster as whole is stable and running.

14. Wait up to 20 minutes and check if the alarm is cleared. Is the alarm cleared?

Yes: Proceed with Step 17.

No: Continue with the next step.

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

Note: Collect the NTP status and ARP tables status.

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