

NTP Authentication Failure

Cloud Execution Environment

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2016–2018. 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
1.1	Alarm Description	1
1.2	Prerequisites	2
2	Procedure	3
2.1	Actions for Solving the Alarm	3



NTP Authentication Failure



1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The NTP Authentication Failure alarm is issued by the Managed Object (MO) `UpstreamNTPServerConnection`. The alarm is issued when NTP service on the virtual Cloud Infrastructure Controller (vCIC) is not able to communicate with one of the upstream NTP servers owing to authentication failure.

The possible alarm causes and the corresponding fault reasons, fault locations, and impacts are described in Table 1.

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
Authentication failure	NTP authentication fails when NTP client of the compute host which hosts the vCIC tries to reach one or several of the upstream servers.	NTP authentication configured incorrectly on upstream NTP servers or on the compute hosts which host the vCICs.	Upstream NTP server key file, for example <code>/etc/ntp.keys</code>	CEE might not have the correct UTC time of day information.
			The NTP server key configuration of the compute host which hosts the vCIC	
			Upstream NTP server NTP configuration file, for example <code>/etc/ntp.conf</code>	

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

The following is the consequence for the node if the alarm is not solved:

- The time on the compute hosts which host the vCICs and other nodes may not be synchronized with UTC time server. Therefore the time on the compute hosts which host the vCICs and other nodes may not have the correct UTC time.
- Reduced redundancy, or complete loss of the NTP service from external sources to CEE. This depends on the number of NTP servers that are working and the number used.

The alarm attributes are listed in Table 2.



Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	2031707
Managed Object Class	UpstreamNTPServerConnection
Managed Object Instance	Region=<name_of_the_region>, CeeFunction=1, Node=<hostname_of_the_node>, UpstreamNTPServerConnection=1
Specific Problem	NTP Authentication Failure
Event Type	other (1)
Probable Cause	realTimeClockFailure (70)
Additional Text	NTP error
Severity	MINOR (5)

1.2 Prerequisites

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

1.2.1 Documents

The following documents are needed to solve the alarm:

- NTP Upstream Server Failure
- Data Collection Guideline

1.2.2 Tools

No tools are required.

1.2.3 Conditions

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

- SSH credentials for the compute host which hosts the vCIC and compute node are available.
- An NTP Authentication Failure alarm is active.



2 Procedure

This section describes the procedure to follow when this alarm is active.

2.1 Actions for Solving the Alarm

If the NTP Upstream Server Failure alarm is also active, follow the instructions in *NTP Upstream Server Failure* OPI to fix the alarm. After that, log on to the compute host which hosts the vCIC, related to the alarm as a normal user, and continue with the following steps:

1. Fetch information from the servers by executing the following command on the compute host which hosts the vCIC:

```
ntpq -c as
```

Example of output from controller node compute-0-6:

ind	assid	status	conf	reach	auth	condition	last_event	cnt
1	29326	9024	yes	yes	none	reject	reachable	2
2	29327	9024	yes	yes	none	reject	reachable	2
3	29328	f61d	yes	yes	ok	sys.peer		1
4	29329	c01c	yes	no ⁽¹⁾	bad ⁽¹⁾	reject		1
5	29330	c01c	yes	yes	ok	candidate		1
6	29331	c011	yes	yes	ok	candidate	mobilize	1

(1) failure indication

The authentication status of the servers is to be interpreted as follows:

Authentication Status	Indication
auth: bad	Failed authentication
auth: ok	Good authentication.
auth: none	No authentication

2. List the upstream stratum level by executing the command:

```
root@compute-0-2:~# ntpq -p
```

Example of output:

remote	refid	st	t	when	poll	reach	delay	offset	jitter
compute-0-6.do main.	10.35.50.5	5	u	66	1024	377	0.295	-0.139	0.497
compute-0-5.do main.	10.35.50.5	5	u	888	1024	376	0.180	0.089	0.107
*10.35.50.5	192.168.50.4	4	u	347	1024	377	0.236	1.920	0.039



seki20-ntp4.k2.	.INIT.	16	u	-	1024	0	0.000	0.000	0.000
192.168.6.1	10.35.50.6	4	u	68	1024	377	0.123	1.631	0.109
google-public-d	10.35.50.6	4	u	251	1024	377	0.256	0.928	0.171

3. List the NTP server configuration on vCIC node:

```
cat /etc/ntp.conf | grep server
```

Output examples:

```
server 10.35.50.5 key 10 burst iburst
server 10.51.40.103 key 10 burst iburst
server 192.168.6.1 key 10 burst iburst
server 8.8.4.4 key 10 burst iburst
```

4. Analyze the printouts according to the following steps:

The two first servers with names starting with `cic-` are the controller peer nodes (the 1st and 2nd in the example). They can be ignored in the analysis.

In the information from Step 1, check the status of the `auth` column. If the status is bad, it indicates an authentication problem with that server.

To find the hostname of the server, compare the printout from Step 1 and Step 2. The servers are listed in the same order in both printouts. The server hostnames or IP addresses are listed in the `remote` column in the printout in Step 2.

To find the IP address of the server, compare printouts from Step 2 and Step 3. In Step 3, the upstream NTP servers IP addresses are listed in the first column. The vCICs are not listed in the printout in Step 3, but the order is the same.

In this example, in Step 1, the fourth server has `auth` status bad, which indicates a problem with authentication.

From Step 2, the conclusion is that the hostname is `seki20-ntp4.k2.`, and in Step 3, the corresponding IP address is `10.51.40.103`.

The conclusion is that the compute hosts, which host the vCICs, have reported authentication failure with the following server in the `/etc/ntp.conf`

```
server 10.51.40.103 key 10 burst iburst
```

5. If the authentication fails, the authentication-related configuration file: `/etc/ntp.keys`, must be checked. Ensure that this matches the configuration on the upstream NTP servers.

- a. If the configurations do not match:

Elevate rights using `sudo`:

- Update the configuration file.
- Restart the NTP service with the following command:
service ntp restart



- b. Try to ping the upstream server which reported the NTP Authentication Failure alarm. Use the command:
`ping <upstream_server_ip>`
 - If the server responds to the ping, the authentication has failed. In this case, match the content in `/etc/ntp.keys` with the configuration in the NTP server.
 - If the server does not respond, the upstream server is down, or there is a network connection issue towards the upstream NTP server. In this case, report the problem to the next level of support and exit this procedure. Job is completed.
6. In case the alarm persists, do the following:
 - Collect all files obtained in Step 1–Step 5.
 - Collect troubleshooting data as described in the [Data Collection Guideline](#).

Note: Alarm logs from Atlas and Linux console as generated from the system when following this OPI.
 - Consult the next level of maintenance support with all collected information.

Further actions are outside the scope of this instruction.
7. The job is completed.