NTP Upstream Server Failure

Cloud Execution Environment

OPERATING INSTRUCTIONS

6/1543-CRA 119 1861/5 Uen A

Contents

1	**Introduction**	**1**
1.1	Alarm Description	1
1.2	Prerequisites	2
2	**Procedure**	**3**
2.1	Actions for Solving the Alarm	3

1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

This is a primary alarm. The alarm is issued by the Managed Object (MO) `UpstreamNTPServerConnection`. The alarm is issued when `NTP Upstream Server Failure` occurs. Upstream failure means that NTP client on vCIC nodes cannot reach one of the upstream servers in the NTP server list.

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
Upstream server not reachable.	Specified compute host which hosts the vCIC cannot reach one of the upstream servers.	• Upstream server down	Upstream NTP server	The time on the compute hosts which host the vCICs and other nodes might be unsynchronized with UTC time server. Therefore the time on the compute host which hosts the vCIC and other nodes might not have the correct UTC time.
		• Network problems	Upstream NTP Server, or the compute host which hosts the vCICs, or router, or switch in the network from the compute host which hosts the vCIC to the upstream NTP servers.	
		• Configuration fault of the compute host which hosts the vCIC	vCIC host	
		• NTP server configuration fault	Upstream NTP server	

Note: An alarm can appear as a result of the 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 are not synchronized with UTC time server and may not have the correct UTC time.
- The impact can be reduced redundancy or complete loss of NTP service from external sources to CEE. This depends on the number of NTP servers that are working and used.

The alarm attributes are listed in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	`193`
Minor Type	`2031709`
Managed Object Class	`UpstreamNTPServerConnection`
Managed Object Instance	`Region=<name_of_the_region>, CeeFunction=1, Node=<hostname_of_the_node>, UpstreamNTPServerConnection=1`
Specific Problem	`NTP Upstream Server 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 Authentication Failure*
- *Data Collection Guideline*

1.2.2 Tools

No tools are required.

1.2.3 Conditions

Before starting this procedure, ensure that the following condition is met:

- SSH credentials for the compute hosts which host the vCICs and the compute host are available.
- An *NTP Upstream Server 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

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

The following example output is taken from a controller node, `compute-0-6`. Do the following:

1. Fetch information from the servers by executing the following command on the compute hosts which host the vCICs:
   `ntpq -c as`
   Example of output:

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	none	sys.peer		1
4	29329	c01c	yes	no(1)	none	reject		1
5	29330	c01c	yes	yes	none	candidate		1
6	29331	c011	yes	yes	none	candidate	mobilize	1

(1) failure indication

2. List the NTP servers information 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.domain.	10.35.50.5	5	u	66	1024	377	0.295	-0.139	0.497

compute-0-5.domain.	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 the compute hosts which host the vCICs with the following command:

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

   The output example is:

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

4. The failure indication of Step 1 shows that `server 4` has the value `no` in the `reach` column. This indicates that the vCIC has general problem to reach its upstream NTP servers.

   If the `auth` column has a value `bad` for any of the servers, debug further according to *NTP Authentication Failure*.

   Check which servers have `no` in the column `reach`. In the example output, `server 4` shows the status `no` in the column `reach`. This means that the compute host which hosts the vCIC is not able to reach upstream `server 4`.

   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, `server 4` has `reach` status `no`, which indicates a problem with the upstream NTP server.

   `Server 4` shown in Step 2 has hostname `seki20-ntp4.k2.`, and the IP address is `10.51.40.103`. Therefore, the vCIC has reported to have upstream server failure with the following servers in the `/etc/ntp.conf`
   `server 10.51.40.103 burst iburst`

5. Test the network connection, using **`ping`** ***`<upstream_server>`*** to verify the network connection from the vCIC to the upstream NTP server.

If there is *no* response from the **`ping`** command, continue with Step 8.

If there is a response from the NTP server, continue with Step 6.

6. Check the authentication status of the NTP servers. Follow the guide below to find out which action to perform.

Authentication Status	Go To	Indication
`auth: bad`	*NTP Authentication Failure*	Failed authentication
`auth: none`	This OPI	No authentication

7. If there is no authentication configured (that is `auth: none`), do the following:

   a. Check the local configuration file

   b. Update the configuration file

   c. Restart the NTP service with the following command:

      ```
      sudo service ntp restart
      ```

   When the issue is fixed, the *NTP Upstream Server Failure* alarm disappears from the alarm list.

8. In case the alarm persists, do the following:

   - Collect all output obtained in Step 1–Step 7.
   - Collect troubleshooting data as described in the *Data Collection Guideline*. For alarm-specific logs, refer to the Table *Data Collection for Alarms and Alerts* 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.

9. The job is completed.