

Control Path Connection Failure

Cloud Execution Environment

OPERATING INSTRUCTIONS

Copyright

© Ericsson AB 2017, 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	2
2.1	Actions	3
	Reference List	7



Control Path Connection Failure



1 Introduction

This instruction concerns alarm handling.

1.1 Alarm Description

The Control Path Connection Failure alarm is issued by the Managed Object (MO) DPN when the connection between the controller node of the Cloud SDN Controller (CSC) and the Cloud SDN Switch (CSS) is lost.

The severity of the alarm is CRITICAL.

Possible alarm causes and fault locations are explained in Table 1.

Table 1 Alarm Causes

Alarm Cause	Description	Fault Reason	Fault Location	Impact
CSS is down	Communication is lost	CSS is administratively shut down or is crashed	CSS	The service provided by the component is degraded or lost
Link between controller node and CSS is down	Network connectivity is lost between controller node and CSS	<ul style="list-style-type: none">• Hardware fault• Network fault	<ul style="list-style-type: none">• Controller host• Switch infrastructure• Ethernet network	The service provided by the component is degraded or lost

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

- The service provided by the component is degraded or lost.

The alarm attributes are listed in Table 2.

Table 2 Alarm Attributes

Attribute Name	Attribute Value
Major Type	193
Minor Type	2162689
Managed Object Class	DPN



Attribute Name	Attribute Value
Managed Object Instance	Region=<name_of_the_region>, Service=SDNc, Alarm=ControlPathConnectionFailure, DPN=<dpn_id>
Specific Problem	SDNc, Heart beat lost between OF Switch and Controller Node
Event Type	communicationsAlarm
Probable Cause	302
Additional Text	:<hw_uuid_of_corresponding_server>
Severity	CRITICAL

1.2 Prerequisites

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

1.2.1 Documents

For more information on SDN alarms, refer to the below SDN documents:

- Alarms, Reference [1] for CSC (controller)
- CSS Troubleshooting Guide, Reference [2] for CSS (switch)

1.2.2 Tools

No tools are required.

1.2.3 Conditions

Before starting this procedure, ensure that access to the vCICs is available.

2 Procedure

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



2.1 Actions

Do the following:

1. Identify the affected compute server:
 - a. Note down the HW UUID from the Additional Text field of the alarm.
 - b. Match the HW UUID to the specific compute server with one of the following tools:

— REST API

For more information refer to the HDS topic List Computer Systems Assigned to a vPOD Using REST API, Reference [3].

— HDS Command Center Manager (CCM) GUI

For more information refer to the HDS topic List Computer Systems Assigned to a vPOD Using GUI, Reference [3].

2. Check the switch.

- a. Check the connection state between CSC and CSS.

Log in to a vCIC and execute the below command to collect port information:

```
ovs-vsctl show
```

```
ovs-vsctl list-ports <bridge_name>
```

- b. Log in to the affected compute server and check the status of CSS:

```
service openvswitch-switch status
```

If CSS is down, restart it.

Note: Restarting CSS causes all VMs to restart.

```
service openvswitch-switch start
```

If the connection is reestablished and the alarm ceases, exit this procedure. Else, continue with Step 3.

3. Check the port.

- a. On the vCIC node hosting the CSC service, check the port status:

```
netstat -antp | grep 6653
```



where 6653 is the default port for messages coming from CSS. Check that port 6653 is in listen mode.

Example output where the port is up:

```
root@cic-1:~# netstat -antp | grep :6653
tcp6          0      0 :::6653          :::*              *
```

Example output where the port is down:

```
root@cic-1:~# netstat -antp | grep :6653
root@cic-1:~#
```

- b. If the port is down, check the status of the sdnc service:

```
crm resource status p_sdnc-service
```

Example output:

```
root@cic-1:~# crm resource status p_sdnc-service
resource p_sdnc-service is running on: cic-1.domain.tld
resource p_sdnc-service is running on: cic-3.domain.tld
resource p_sdnc-service is running on: cic-2.domain.tld

root@cic-1:~# /etc/init.d/sdnc-service status
SDN controller services Running..
```

If the service is in ERROR state, restart it:

```
crm resource restart p_sdnc-service
```

Restart can take about 3-5 minutes. Wait for 5 minutes before executing any other command.

The following scenarios are possible:

- If restart is successful, the connection is reestablished, and the alarm ceases, exit this procedure.
- If restart is successful, but the alarm remains, continue with Step c.
- If restart fails, continue with Step 5.

- c. Check if E-ODL is up and running:

```
display app-status [--all <all>]
```

Example output:

```
root@cic-1:~# /etc/init.d/sdnc-service comcli
```




```
cli>display app-status
Enter password for user cscadm:
Timestamp: Thu Jul 06 08:28:53 GMT+01:00 2017
Node IP Address: 192.168.70.2
  INTERFACE_SERVICE : OPERATIONAL
  OPENFLOW          : ERROR
  ITM                : OPERATIONAL
  DATASTORE_SERVICE : OPERATIONAL
  SCF_SERVICE        : OPERATIONAL
  ELAN_SERVICE       : OPERATIONAL
Node IP Address: 192.168.70.3
  INTERFACE_SERVICE : OPERATIONAL
  OPENFLOW          : OPERATIONAL
  ITM                : OPERATIONAL
  DATASTORE_SERVICE : OPERATIONAL
  SCF_SERVICE        : OPERATIONAL
  ELAN_SERVICE       : OPERATIONAL
Node IP Address: 192.168.70.4
  INTERFACE_SERVICE : OPERATIONAL
  OPENFLOW          : OPERATIONAL
  ITM                : OPERATIONAL
  DATASTORE_SERVICE : OPERATIONAL
  SCF_SERVICE        : OPERATIONAL
  ELAN_SERVICE       : OPERATIONAL
```

If any service is in ERROR state, restart CSC:

```
crm resource restart clone_p_sdnc-service
```

4. Check the underlying connectivity and collect the below information for diagnostic purposes.

On the CSC switch node, check whether connectivity exists with CSC by validating that the port and the IP address are available:

```
telnet <csc_ip> 6653
```

where <csc_ip> is the IP address of the vCIC node hosting the CSC service.

An example output is:

Example output where connectivity exists:

```
root@cic-2:~# telnet 192.168.40.31 6653
Trying 192.168.40.31...
Connected to 192.168.40.31.
Escape character is '^['.
```

where 192.168.40.31 is the IP address of the vCIC node.



Example output where there is no connectivity:

```
root@cic-2:~# telnet 192.168.40.31 6653
Trying 192.168.40.31...
telnet: Unable to connect to remote host: Connection refused
```

This can indicate an underlay fault. Refer to alarm topic `LostConnection` in the HDS documentation, Reference [3], and continue with Step 5.

5. Collect further troubleshooting data as described in the [Data Collection Guideline](#).
6. Contact the next level of maintenance support.

Further actions are outside the scope of this instruction.

7. The job is completed.



Reference List

- [1] Alarms, 1/198 22-AXD 101 08/6-V1
- [2] CSS Troubleshooting Guide, 154 51-AXT 901 11/2-V1
- [3] Hyperscale Datacenter System 8000 Customer Documentation, 2/1551-LZN 901 5032