

# Data 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

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Alarm Description	1
1.2	Prerequisites	3
<b>2</b>	<b>Procedure</b>	<b>3</b>
2.1	Actions	4
2.2	Collect Troubleshooting Data	7
	<b>Reference List</b>	<b>8</b>



Data Path Connection Failure



# 1 Introduction

This instruction concerns alarm handling.

## 1.1 Alarm Description

This section describes the Data Path Connection Failure alarm.

The Data Path Connection Failure alarm is issued by the Managed Object (MO) DstDPN when the data path connectivity is lost between:

- The Data Plane Nodes (DPNs)
- The DPN and Data Center Gateway (DC-GW)
- The DPN and the HW VXLAN Tunnel End Point (VTEP)

**Note:** The Cloud SDN Controller (CSC) generates this alarm only if the Cloud SDN Switch (CSS) switch port failure affects DPN connectivity.

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
Data path connectivity is lost between: <ul style="list-style-type: none"><li>• DPNs</li><li>• DPN and DC-GW</li><li>• DPN and HW-VTEP</li></ul>	The data path connectivity is lost between a pair of CSSs.	<ul style="list-style-type: none"><li>• Hardware fault</li><li>• Network fault</li></ul>	CSS	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	2162690
Managed Object Class	DstDPN
Managed Object Instance	<p>Region=&lt;name_of_the_region&gt;, Service=SDNc, Alarm=DataPathConnectionFailure, SrcDPN=&lt;dpn_id&gt; DstDPN=&lt;dpn_id&gt;<sup>(1)</sup></p> <p>or</p> <p>Region=&lt;name_of_the_region&gt;, Service=SDNc, Alarm=DataPathConnectionFailure srcDevice=&lt;openflow_source_device_id&gt; -dstDevice=&lt;openflow_ip_address&gt; _ipv4Address=Ipv4Address _value=&lt;ip_address&gt; -tunnelTypeVXLAN<sup>(2)</sup></p> <p>or</p> <p>Region=&lt;name_of_the_region&gt;, Service=SDNc, Alarm=DataPathConnectionFailure srcDevice=&lt;openflow_source_device_id&gt; -dstDevice=&lt;hwvtep_uuid&gt; -tunnelTypeVXLAN<sup>(3)</sup></p>
Specific Problem	SDNc, data path connectivity between DPNs is lost
Event Type	communicationsAlarm
Probable Cause	302



Attribute Name	Attribute Value
Additional Text	:<hw_uuid_of_corresponding_server>:<hw_uuid_of_corresponding_server> <sup>(1)</sup> or :<hw_uuid_of_corresponding_server>:IpAddress <sup>(2)</sup> or :<hw_uuid_of_corresponding_server> <sup>(3)</sup>
Severity	CRITICAL

(1) When the connectivity is lost between DPNs.

(2) When the connectivity is lost between DPN and DC-GW.

(3) When the connectivity is lost between DPN and HW-VTEP.

## 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 following 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

Not applicable.

## 2 Procedure

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



- If the connectivity is lost between the DPNs, see Section 2.1.1 on page 4.
- If the connectivity is lost between a DPN and the DC-GW, see Section 2.1.2 on page 5.
- If the connectivity is lost between a DPN and the HW-VTEP, see Section 2.1.3 on page 6.

## 2.1 Actions

### 2.1.1 Actions for Data Path Connection Failure Between DPNs

Do the following:

1. Identify the affected compute servers:
  - a. Note down the HW UUIDs from the Additional Text field of the alarm.
  - b. Match the HW UUIDs 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. On source and destination CSS hosts, check the status of CSS.
  - a. **service openvswitch-switch status**  
If CSS is down, restart it.  
**Note:** Restarting CSS causes all VMs to restart.  
**service openvswitch-switch start**
  - b. Check whether data connectivity between the source and destination CSSs is operational:

**ping <destination\_css\_ip>**

An example output where the ping is successful is shown below.





```
cic-1:~ # ping 10.184.22.13
PING 10.184.22.13 (10.184.22.13) 56(84) bytes of data.
64 bytes from 10.184.22.13: icmp_seq=1 ttl=254 time=1.03 ms
64 bytes from 10.184.22.13: icmp_seq=2 ttl=254 time=0.867 ms
64 bytes from 10.184.22.13: icmp_seq=3 ttl=254 time=0.780 ms
^C
--- 10.184.22.13 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.780/0.895/1.038/0.107 ms
```

An example output where the ping fails is shown below.

```
cic-1:~ # ping 10.184.22.99
PING 10.184.22.99 (10.184.22.99) 56(84) bytes of data.
^C
--- 10.184.22.99 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5038ms
```

If the ping fails, this can indicate an underlay fault. Refer to alarm topic `LostConnection` in the HDS documentation, Reference [3], and continue with Section 2.2 on page 7.

If the connection is reestablished and the alarm ceases, exit this procedure. Else, continue with Section 2.2 on page 7.

## 2.1.2 Actions for Data Path Connection Failure Between DPN and DC-GW

Do the following:

1. Identify the affected compute servers:
  - a. Note down the HW UUID of the source device and the IP address of the destination device from the alarm output.
  - 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. On source and destination CSS hosts, check the status of CSS.
  - a. **service openvswitch-switch status**

If CSS is down, restart it.

**Note:** Restarting CSS causes all VMs to restart.



```
service openvswitch-switch start
```

- b. Check whether data connectivity between the CSS and the DC-GW is operational:

```
ping <destination_dc-gw_ip>
```

If the ping fails, this can indicate an underlay fault. Refer to alarm topic LostConnection in the HDS documentation, Reference [3], and continue with Section 2.2 on page 7.

If the connection is reestablished and the alarm ceases, exit this procedure. Else, continue with Section 2.2 on page 7.

### 2.1.3 Data Path Connection Failure Between DPN and HW-VTEP

Do the following:

1. Identify the affected compute servers:

- a. From the alarm output, note down the following data:

- HW UUID of the source device
- Node ID of the destination device
- Name of the destination HW-VTEP device

An example for the HW-VTEP device name is the following:

```
hwvtep://uuid/<node_id>/physicalswitch/⇒  
<device_name>
```

- 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. On source and destination CSS hosts, check the status of CSS.

- a. **service openvswitch-switch status**

If CSS is down, restart it.

**Note:** Restarting CSS causes all VMs to restart.



```
service openvswitch-switch start
```

- b. Check whether data connectivity between the CSS and the HW-VTEP is operational:

```
ping <destination_hwvtep_device_ip>
```

If the ping fails, this can indicate an underlay fault. Refer to alarm topic `LostConnection` in the HDS documentation, Reference [3], and continue with Section 2.2 on page 7.

If the connection is reestablished and the alarm ceases, exit this procedure. Else, continue with Section 2.2 on page 7.

## 2.2 Collect Troubleshooting Data

If the connection is not reestablished, follow the below steps:

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

Further actions are outside the scope of this instruction.

3. 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