


# **Dell SmartFabric OS10 System Log Message Reference Guide**

Release 10.5.3.2

## Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

|   |           |
|---|-----------|
| <b>Chapter 1: Revision history.....</b>                               | <b>6</b>  |
| <b>Chapter 2: About this guide.....</b>                               | <b>7</b>  |
| Audience.....   | 7         |
| Conventions.....  | 7         |
| Documentation Feedback.....   | 7         |
| Related Documents.....  | 8         |
| <b>Chapter 3: System log messages overview.....</b>                   | <b>9</b>  |
| System events and alarms.....   | 9         |
| Configure custom severity profile.....                                | 10        |
| System logging over TLS.....  | 11        |
| View system logs.....   | 13        |
| <b>Chapter 4: ACL system log message reference.....</b>               | <b>15</b> |
| <b>Chapter 5: AFS system log message reference.....</b>               | <b>17</b> |
| <b>Chapter 6: ALM_ACCNT_MAC system log message reference.....</b>     | <b>18</b> |
| <b>Chapter 7: ALM_CLOCK system log message reference.....</b>         | <b>19</b> |
| <b>Chapter 8: BFD system log message reference.....</b>               | <b>20</b> |
| <b>Chapter 9: BGP system log message reference.....</b>               | <b>21</b> |
| <b>Chapter 10: CMS system log message reference.....</b>              | <b>26</b> |
| <b>Chapter 11: Configuring LLFC system log message reference.....</b> | <b>27</b> |
| <b>Chapter 12: DCBX system log messages.....</b>                      | <b>28</b> |
| <b>Chapter 13: DENIED_ARP system log message reference.....</b>       | <b>29</b> |
| <b>Chapter 14: DOT1X system log message reference.....</b>            | <b>30</b> |
| <b>Chapter 15: DYNAMIC_MGMT system log message reference.....</b>     | <b>31</b> |
| <b>Chapter 16: EQM system log message reference.....</b>              | <b>32</b> |
| <b>Chapter 17: ETL system log message reference.....</b>              | <b>36</b> |

|   |    |
|---|----|
| Chapter 18: EVPN system log message reference.....                                    | 37 |
| Chapter 19: FC_SVCS system log message reference.....                                 | 38 |
| Chapter 20: FCOE system log message reference.....                                    | 40 |
| Chapter 21: FEFD system log message reference.....                                    | 42 |
| Chapter 22: IGMP system log message reference.....                                    | 43 |
| Chapter 23: IP system log message reference.....                                      | 44 |
| Chapter 24: IPv6 system log message reference.....                                    | 45 |
| Chapter 25: ISCSI system log message reference.....                                   | 46 |
| Chapter 26: LACP system log message reference.....                                    | 48 |
| Chapter 27: LADF system log message reference.....                                    | 49 |
| Chapter 28: LB system log message reference.....                                      | 50 |
| Chapter 29: LLDP system log message reference.....                                    | 51 |
| Chapter 30: MGMT_CLISH system log message reference.....                              | 52 |
| Chapter 31: SFS host tracking system log message reference.....                       | 53 |
| Chapter 32: Symmetric hashing system log message reference.....                       | 54 |
| Chapter 33: SyncE ESMC system log message reference.....                              | 55 |
| Chapter 34: SYSTEM_MODE_CHANGE system log message reference.....                      | 57 |
| Chapter 35: SupportAssist - CloudIQ data collection system log message reference..... | 58 |
| Chapter 36: MLD system log message reference.....                                     | 59 |
| Chapter 37: NDM system log message reference.....                                     | 60 |
| Chapter 38: PBR match access-list system log message reference.....                   | 61 |
| Chapter 39: OPEN_FLOW system log message reference.....                               | 62 |
| Chapter 40: OSPFv2 system log message reference.....                                  | 63 |

|  |    |
|--|----|
| Chapter 41: OSPFv3 system log message reference.....                   | 65 |
| Chapter 42: Port security system log message reference.....            | 67 |
| Chapter 43: PIM system log message reference.....                      | 68 |
| Chapter 44: PKI certificate system log message reference.....          | 69 |
| Chapter 45: PTP system log message reference.....                      | 74 |
| Chapter 46: QoS system log message reference.....                      | 76 |
| Chapter 47: RAGUARD_EVENT system log message reference.....            | 77 |
| Chapter 48: RAGUARD system log message reference.....                  | 78 |
| Chapter 49: Routemap with match ACL system log message reference.....  | 79 |
| Chapter 50: Scale VLAN profile system log message reference.....       | 80 |
| Chapter 51: Static and dynamic route system log message reference..... | 83 |
| Chapter 52: SA system log message reference.....                       | 84 |
| Chapter 53: Scheduled reload system log message reference.....         | 85 |
| Chapter 54: STATIC_MGMTsystem log message reference.....               | 86 |
| Chapter 55: STP system log message reference.....                      | 87 |
| Chapter 56: UFD system log message reference.....                      | 88 |
| Chapter 57: USER_ROLE_CHANGED system log message reference.....        | 89 |
| Chapter 58: Delay restore port system log message reference.....       | 90 |
| Chapter 59: VLT system log message reference.....                      | 91 |
| Chapter 60: VRF system log message reference.....                      | 94 |
| Chapter 61: VXLAN system log message reference.....                    | 95 |
| Chapter 62: IFM system log message reference.....                      | 96 |
| Index.....   | 98 |

# Revision history

This table provides an overview of the changes in this guide.

**Table 1. Revision history**

| Release  | Revision        | Description   |
|----------|-----------------|---|
| 10.5.2.6 | A00 (June 2021) | Initial release   |
| 10.5.3.0 | A01 (Sep 2021)  | Included System log messages corresponding to the following 10.5.3.0 features: <ul style="list-style-type: none"><li>• BGP un-numbered</li><li>• LACP Individual</li><li>• Port security</li><li>• Scheduled reload</li><li>• Z9432F north-bound external interfaces support</li><li>• PKI certificate validation</li><li>• Symmetric hashing</li><li>• IPv6 RA options for DNS configuration</li><li>• Port channel (Wider range ID, 1 to 2000 support)</li><li>• syncE ESMC</li></ul> |
| 10.5.3.2 | A01 (Dec 2021)  | Included System log messages corresponding to the following 10.5.3.2 features: <ul style="list-style-type: none"><li>• SFS host tracking</li><li>• SupportAssist - CloudIQ data collection</li></ul>  |

## About this guide

This guide is intended for system administrators who are responsible for configuring and maintaining networks. It covers the following details:

- Information on system events and alarms.
- Lists the System log messages corresponding to various protocols and services that are generated by SmartFabric Dell OS10.
- Provides Description for each System log message and the Recommended action that you can take to mitigate the System log message.
- Specifies the Severity of each System log message.

To use this guide, you must have a good knowledge of Layer 2 (L2) and Layer 3 (L3) networking technologies.

This document may contain language that is not consistent with current guidelines of Dell Technologies. There are plans to update this document over subsequent releases to revise the language accordingly.

### Topics:

- [Audience](#)
- [Conventions](#)
- [Documentation Feedback](#)
- [Related Documents](#)

## Audience

This document is intended for system administrators who are responsible for configuring and maintaining networks and assumes knowledge in Layer 2 (L2) and Layer 3 (L3) networking technologies.

## Conventions

This guide uses the following conventions to describe command syntax.

|                         |   |
|-------------------------|---|
| <b>Keyword</b>          | Keywords are in Courier (a monospaced font) and must be entered in the CLI as listed. |
| <b><i>parameter</i></b> | Parameters are in italics and require a number or word to be entered in the CLI.      |
| <b>{X}</b>              | Keywords and parameters within braces must be entered in the CLI.                     |
| <b>[X]</b>              | Keywords and parameters within brackets are optional.                                 |
| <b>x y</b>              | Keywords and parameters separated by a bar require you to choose one option.          |

## Documentation Feedback

Dell Technologies strives to provide accurate and comprehensive documentation and welcomes your suggestions and comments. You can provide feedback in the following ways:

- Online feedback form—Rate the documentation or provide your feedback on any of our documentation pages at [www.dell.com/support](http://www.dell.com/support).
- Email—Send your feedback to [networkingpub.feedback@dell.com](mailto:networkingpub.feedback@dell.com). Include the document title, release number, chapter title, and section title of the text corresponding to the feedback.

To get answers to your questions related to Dell SmartFabric OS10 through email, chat, or call, please visit our [Technical Support](#) page.

# Related Documents

Dell SmartFabric OS10 is part of various networking solution deployments including PowerEdge MX, VxRail, and so on. The following tables list all the available documentation for Dell SmartFabric OS10.

**Table 2. SmartFabric OS10 Documentation**

| Related Documentation  | Description  | Link  |
|--|--|---|
| <ul style="list-style-type: none"><li>• <i>Dell SmartFabric OS10 Upgrade and Downgrade Guide</i></li><li>• <i>Dell SmartFabric OS10 Quick Start Guide</i></li><li>• <i>Dell SmartFabric OS10 Release Notes</i></li><li>• <i>Dell SmartFabric OS10 Security Guide</i></li><li>• <i>Dell SmartFabric OS10 User Guide</i></li></ul> | Dell SmartFabric OS10 Documentation.   | <a href="#">Dell EMC Networking OS10 Info Hub</a> |
| Dell Technologies Networking Solutions Portfolio   | Technical content about the Dell Technologies networking solutions portfolio that enables you to meet the demands of modern workloads, from the edge to the core to the cloud. | <a href="#">Networking Solutions</a>              |



# System log messages overview

This chapter provides an overview of the system log messages supported in Dell SmartFabric OS10.

## Topics:

- [System events and alarms](#)
- [System logging over TLS](#)
- [View system logs](#)

## System events and alarms

An event notifies you of a change or situation in the system that you might be interested in. An alarm indicates that the system has entered an abnormal state and may require immediate action.

Events are classified as follows:

- **Stateless events**—One-time notifications about the system condition, for example, ACL updates, firewall policy update, and so on.
- **Stateful events**—Events that are raised when the abnormal situation arises, and cleared when the situation returns to normal. These types of events are called alarms.

Events can have one of the following severities:

- **CRITICAL**—A critical condition exists and requires immediate action. A critical event may trigger if one or more hardware components fail, or one or more hardware components exceed temperature thresholds.
- **MAJOR**—A major error had occurred and requires escalation or notification. For example, a major alarm may trigger if an interface failure occurs, such as a port channel being down.
- **MINOR**—A minor error or noncritical condition occurred that, if left unchecked, might cause system service interruption or performance degradation. A minor alarm requires monitoring or maintenance.
- **WARNING**—A warning condition was observed, but it may or may not result in an error condition.
- **INFORMATIONAL**—An informational event had occurred, but it does not impact performance.

Out of memory, temperature crossing a critical point, and so on, are examples of conditions when the system triggers an alarm. After the system recovers from the condition, the alarms are cleared.

All stateful events of severity level CRITICAL, MAJOR, MINOR, or WARNING trigger alarms. However, you can customize the severity of events or turn off event notification using Severity profiles.

Triggered alarms are in one of these states:

- **Active**—Alarm is raised and is currently active.
- **Acknowledged**—Alarm is raised; the user is aware of the situation and acknowledged the alarm. This alarm does not impact the overall health of the system or the system LED.

Some alarms go directly from active to cleared state and require little-to-no administrative effort. You must acknowledge or investigate alarms with a high severity.

OS10 stores all Active and Acknowledged alarms in the Current Alarm List (CAL), and archives all past events in the Event History List (EHL).

Alarms in the CAL are cleared after a reload.

The EHL is persistent and retains the archived events after a reload, reboot, or upgrade. The EHL can store a maximum of 86,000 events or 30 days of events, whichever is earlier.

The system LED that indicates the status of the switch is based on the severity of the alarms in the CAL and it turns:

- Red—For CRITICAL or MAJOR alarms
- Amber—For MINOR or WARNING alarms
- Green—No alarms

## Configure custom severity profile

To modify the severity of events or disable event notification:

Your user account must have any one of the following privileges: System admin (sysadmin), security admin (secadmin), or network admin (netadmin).

1. Use the `dir` command to view the list of available severity profiles in the `severity-profile://` partition.

```
OS10# dir severity-profile
Date (modified)      Size (bytes)  Name
-----
2019-03-27T15:24:06Z  46741        default.xml
2019-04-01T11:22:33Z  456          custom.xml
```

2. Copy one of the available severity profiles to a remote host.

```
OS10# copy severity-profile://default.xml scp://username:password@a.b.c.d/dir-path/
mySevProf.xml
```

3. Modify the .xml file with changes as required.

**NOTE:** When you modify the xml file, you must select one of the following severities:

- CRITICAL
- MAJOR
- MINOR
- WARNING
- INFORMATIONAL

Following is a sample of the .xml file. you can use Notepad++ to make modifications to his .xml file:

```
<?xml version="1.0" encoding="UTF-8"?>

<events>
<event
name="L2_SERV_LACP_CMS_CPS_SEND_FAIL"
severity="INFORMATIONAL"
enable="true"
/>
<event
name="L2_SERV_LACP_STACK_CPS_SEND_FAIL"
severity="INFORMATIONAL"
enable="true"
/>
<event
name="L2_SERV_LACP_CMS_CPS_RECV_FAIL"
severity="INFORMATIONAL"
enable="true"
/>
<event
name="L2_SERV_LACP_STACK_CPS_RECV_FAIL"
severity="INFORMATIONAL"
```

If you want OS10 to generate the event, set the Enable flag to `true`. To turn off event notification, set the Enable flag to `false`.

If you enter invalid values, the `event severity-profile` command fails.


4. Copy the custom profile to the OS10 switch.

```
OS10# copy scp://username:password@a.b.c.d/dir-path/mySevProf.xml severity-profile://
mySevProf_1.xml
```

When you copy the custom profile, you must update the name of the custom profile. You cannot use the same name as the default profile (`default.xml`) or the active profile (`mySevProf.xml`).

5. Apply the custom severity profile on the switch.

```
OS10# event severity-profile mySevProf_1.xml
```

 **NOTE:** You must restart the switch for the changes to take effect.

6. Restart the switch.

```
OS10# reload
```

7. Use the `show event severity-profile` command to view the custom profile that is active.

```
OS10# show event severity-profile
Severity Profile Details
-----
Currently Active      : default
Active after restart : mySevProf_1.xml
```

## System logging over TLS

To provide enhanced security and privacy in the logged system messages sent to a syslog server, you can use the Transport Layer Security (TLS) protocol. System logging over TLS encrypts communication between an OS10 switch and a configured remote logging sever, including:

- Performing mutual authentication of a client and server using public key infrastructure (PKI) certificates
- Encrypting the entire authentication exchange so that neither user ID nor password is vulnerable to discovery, and that the data is not modified during transport

### Configuration notes

System logging over TLS requires that:

- X.509v3 PKI certificates are configured on a certification authority (CA) and installed on the switch. Both the switch and syslog server exchange a public key in a signed X.509v3 certificate to authenticate each other.
- You configure a security profile for system logging.

### Configure system logging over TLS

1. Copy an X.509v3 certificate created by a CA server using a secure method, such as SCP or HTTPS. Then install the trusted CA certificate in EXEC mode.

```
crypto ca-cert install ca-cert-filepath [filename]
```

- *ca-cert-filepath* specifies the local path to the downloaded certificate; for example, `home://CAcert.pem` or `usb://CA-cert.pem`.
  - *filename* specifies an optional filename that the certificate is stored under in the OS10 trust-store directory. Enter the filename in the *filename.crt* format.
2. Obtain an X.509v3 host certificate from the CA server:
    - a. Create a private key and generate a certificate signing request for the switch.
    - b. Copy the CSR file to the CA server for signing.
    - c. Copy the CA-signed certificate to the home directory on the switch.
    - d. Install the host certificate:

```
crypto cert install cert-file home://cert-filepath key-file {key-path | private}
[password passphrase] [fips]
```

When you install an X.509v3 certificate-key pair:

- Both take the name of the certificate. For example, if you install a certificate using:

```
OS10# crypto cert install cert-file home://Dell_host1.pem key-file home://abcd.key
```

The certificate-key pair is installed as `Dell_host1.pem` and `Dell_host1.key`. In configuration commands, refer to the pair as `Dell_host1`. When you configure a security profile, you would enter `Dell_host1` in the `certificate certificate-name` command.

- For security reasons, because the key file contains private key information, it is copied to a secure location in the OS10 file system and deleted from its original location specified in the `key-file key-path` parameter.

**NOTE:** `fips` installs the certificate-key pair as FIPS-compliant. Enter `fips` to install a certificate-key pair that is used by a FIPS-aware application, such as Syslog over TLS. If you do not enter `fips`, the certificate-key pair is stored as a non-FIPS-compliant pair.

You determine if the certificate-key pair is generated as FIPS-compliant. Do not use FIPS-compliant certificate-key pairs outside of FIPS mode. When FIPS mode is enabled, you can still generate CSRs for non-FIPS certificates for use with non-FIPS applications. Be sure to install these certificates as non-FIPS with the `crypto cert install` command.

3. Configure a security profile for system logging over TLS using an X.509v3 certificate.

- a. Create a Syslog security profile in CONFIGURATION mode.

```
crypto security-profile profile-name
```

- b. Assign an X.509v3 certificate and private key pair to the security profile in SECURITY-PROFILE mode. For `certificate-name`, enter the name of the certificate-key pair as it appears in the `show crypto certs` output without the `.pem` extension.

```
certificate certificate-name
exit
```

- c. Create a system logging-specific profile in CONFIGURATION mode.

```
logging security-profile profile-name
```

Where `profile-name` is the name of the Syslog security profile created in Step 2a with the `crypto security-profile profile-name` command. You cannot delete a crypto server profile if it is configured for a logging server.

If you reconfigure `crypto security profile-name`, configured Syslog TLS servers are automatically updated to use the new certificate-key pair used by the new profile.

If you reconfigure the certificate assigned to a crypto security profile, Syslog TLS servers are automatically updated to use new certificate-key pair.

If you delete a certificate from a configured crypto security profile, system logging over TLS fails. A host certificate is required for the protocol exchange with an external device.

4. Configure a remote TLS server to receive system messages in CONFIGURATION mode.

```
logging server {ipv4-address | ipv6-address} tls [port-number]
[severity severity-level] [vrf {management | vrf-name}]
```

### Example: Configure Syslog over TLS

```
OS10# copy tftp://CAadmin:secret@172.11.222.1/cacert.pem home://cacert.pem
```

```
OS10# crypto ca-cert install home://cacert.pem
Processing certificate ...
Installed Root CA certificate
CommonName = Certificate Authority CA
IssuerName = Certificate Authority CA
```

```
OS10# show crypto ca-certs
```

```
-----
| Locally installed certificates          |
-----
cacert.crt
```

```
OS10# crypto cert generate request cert-file home://clientreq.pem key-file home://
clientkey.pem cname "Top of Rack 6" altname "IP:10.0.0.6 DNS:tor6.dell.com" email
admin@dell.com organization "Dell EMC" orgunit Networking locality "Santa Clara" state
California country US length 2048
Processing certificate ...
Successfully created CSR file /home/admin/clientreq.pem and key
```

```

OS10# copy home://clientreq.pem scp://CAadmin:secret@172.11.222.1/clientreq.pem

OS10# copy scp://CAadmin:secret@172.11.222.1/clientcert.pem home://clientcert.pem
OS10# copy scp://CAadmin:secret@172.11.222.1/clientkey.pem home://clientkey.pem

OS10# crypto cert install cert-file home://clientcert.pem key-file home://clientkey.pem
Processing certificate ...
Certificate and keys were successfully installed as "clientcert.crt" that may be used in
a security profile. CN = 10.0.0.6

OS10# show crypto cert
-----
| Installed non-FIPS certificates |
-----
clientcert.crt
-----
| Installed FIPS certificates |
-----

OS10(config)# crypto security-profile dellprofile
OS10(config-sec-profile)# certificate clientcert
OS10(config-sec-profile)# exit
OS10(config)# logging security-profile dellprofile
OS10(config)# logging server 10.11.86.139 tls
OS10(config)# do show running-configuration logging
!
logging security-profile dellprofile
logging server 10.11.86.139 tls 514

```

## View system logs

The system log-file contains system event and alarm logs.

Use the `show trace` command to view the current syslog file. All event and alarm information is sent to the syslog server, if one is configured.

The `show logging` command accepts the following parameters:

- `log-file` — Provides a detailed log including both software and hardware saved to a file.
- `process-names` — Provides a list of all processes currently running which can be filtered based on the process-name.

### View logging log-file

```

OS10# show logging log-file
Jun  1 05:01:46 %Node.1-Unit.1:PRI:OS10 %log-notice:ETL_SERVICE_UP: ETL service
is up
Jun  1 05:02:06 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_UNIT_DETECTED: Unit pres
ent:Unit 1#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_PSU_DETECTED: Power Supp
ly Unit present:PSU 1#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_PSU_DETECTED: Power Supp
ly Unit present:PSU 2#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_FAN_TRAY_DETECTED: Fan t
ray present:Fan tray 1#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_FAN_TRAY_DETECTED: Fan t
ray present:Fan tray 2#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-notice:EQM_FAN_TRAY_DETECTED: Fan t
ray present:Fan tray 3#003
Jun  1 05:02:09 %Node.1-Unit.1:PRI:OS10 %log-crit:EQM_FAN_AIRFLOW MISMATCH: MAJO
R ALARM: FAN AIRFLOW MISMATCH: SET: One or more fans have mismatching or unknown
airflow directions#003
Jun  1 05:02:10 %Node.1-Unit.1:PRI:OS10 %log-notice:NDM_SERVICE_UP: NDM Service
Ready!
Jun  1 05:02:10 %Node.1-Unit.1:PRI:OS10 %log-notice:SU_SERVICE_UP: Software upgr
ade service is up:software upgrade service up
--More--

```

```

OS10# show logging log-file
Jan  4 19:13:17 OS10 usb_monitor: Node.1-Unit.1:PRI:notice %Dell EMC (OS10) %log-

```

```

notice:USB_DEVICE_INSERTED: Vendor: Linux_3.16.39_ehci_hcd Product: EHCI_Host_Controller
Serial: 0000:00:16.0
Jan  4 19:13:17 OS10 usb_monitor: Node.1-Unit.1:PRI:notice %Dell EMC (OS10) %log-
notice:USB_DEVICE_INSERTED: Vendor: 8087 Product: 07db Serial: unknown
Jan  4 19:13:18 OS10 dn_dot1x[900]: Node.1-Unit.1:PRI:notice [os10:trap], %Dell EMC
(OS10) %log-notice:DOT1X_PDU_RX_FAIL: PDU Reception Failed Kernel Index 1
Jan  4 19:13:20 OS10 dn_etl[917]: Node.1-Unit.1:PRI:notice [os10:event], %Dell EMC
(OS10) %log-notice:ETL_SERVICE_UP: ETL service is up
Jan  4 19:13:50 OS10 dn_eqm[1754]: Node.1-Unit.1:PRI:notice [os10:notify], %Dell EMC
(OS10) %log-notice:EQM_UNIT_DETECTED: Unit present unit 1
Jan  4 19:13:50 OS10 dn_eqm[1754]: Node.1-Unit.1:PRI:notice [os10:publish], %Dell EMC
(OS10) %log-notice:EQM_PSU_DETECTED: Power supply unit present PSU 1
Jan  4 19:13:50 OS10 dn_eqm[1754]: Node.1-Unit.1:PRI:notice [os10:publish], %Dell EMC
(OS10) %log-notice:EQM_PSU_DETECTED: Power supply unit present PSU 2
Jan  4 19:13:50 OS10 dn_eqm[1754]: Node.1-Unit.1:PRI:notice [os10:publish], %Dell EMC
(OS10) %log-notice:EQM_FAN_TRAY_DETECTED: Fan tray present fan tray 1
Jan  4 19:13:50 OS10 dn_eqm[1754]: Node.1-Unit.1:PRI:notice [os10:publish], %Dell EMC
(OS10) %log-notice:EQM_FAN_TRAY_DETECTED: Fan tray present fan tray 2
Jan  4 19:13:50 OS10 dn_eqm[1754]: Node.1-Unit.1:PRI:notice [os10:publish], %Dell EMC
(OS10) %log-notice:EQM_FAN_TRAY_DETECTED: Fan tray present fan tray 3
Jan  4 19:13:50 OS10 dn_eqm[1754]: Node.1-Unit.1:PRI:notice [os10:publish], %Dell EMC
(OS10) %log-notice:EQM_FAN_TRAY_DETECTED: Fan tray present fan tray 4
Jan  4 19:13:50 OS10 dn_eqm[1754]: Node.1-Unit.1:PRI:alert [os10:alarm], %Dell EMC
(OS10) %log-alert:EQM_MORE_PSU_FAULT: More power supply unit (PSU) fault psu 1 is not
working correctly
Jan  4 19:13:52 OS10 dn_eqm[1754]: Node.1-Unit.1:PRI:notice [os10:notify], %Dell EMC
(OS10) %log-notice:EQM_UNIT_CHECKIN: Unit check-in detected unit 1 (type S5148F-ON
48x25GbE, 6x100GbE QSFP28 Interface Module)
--More--

```

## View logging process names

```

OS10# show logging process-names
dn_alm
dn_app_vlt
dn_app_vrrp
dn_bgp
dn_dot1x
dn_eqa
dn_eqm
dn_eth_drv
dn_etl
dn_i3
dn_ifm
dn_infra_afs
dn_issu
dn_l2_services
dn_l2_services_
dn_l2_services_
dn_l2_services_
dn_l2_services_
dn_l3_core_serv
dn_l3_service
dn_lacp
dn_lldp
dn_mgmt_entity_
--More--

```

Following are the descriptions for a couple of processes:

- dn\_bgp - The dn\_bgp is the process that manages the Border gateway protocol.
- dn\_ifm - The dn\_ifm is the process that manages the interfaces.

The following chapters describe system log messages for various protocols and the recommended actions to address them.

## ACL system log message reference

This section lists the messages that are generated by the ACL process.

**Table 3. OS10 ACL system log messages**

| System log message  | Severity      | Description  | Recommended action  |
|---|---------------|--|---|
| %ROUTE_MAP_MATCH_PARAM: Route-map <rmap-name>   | Informational | Match address based on ACL is not applicable for Routing modules in VRF <vrf-name>."   | No action required.   |
| %ACL_TABLE_FULL: ACL table full   | Informational | The ACL TCAM space is of fixed size based on each platform. The system log is generated when there is no space left to program additional rules in the TCAM. This could happen when a new application is started with the TCAM space being full already. | Use the <code>show acl-table-usage detail</code> command to identify the list of applications that are consuming the TCAM space. Based on the application usage, you must disable the other or unused applications. For more details on the <code>show acl-table-usage detail</code> , see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/view-acl-table-utilization-report?guid=guid-cd4a59db-5ccc-404f-9cdb-70181814dde3&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/view-acl-table-utilization-report?guid=guid-cd4a59db-5ccc-404f-9cdb-70181814dde3&amp;lang=en-us</a> . For configuring or disabling the TCAM rules, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/quality-of-service?guid=guid-f52a9db8-3f2f-497c-a517-a79e343271e0&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/quality-of-service?guid=guid-f52a9db8-3f2f-497c-a517-a79e343271e0&amp;lang=en-us</a> . |
| %ACL_TABLE_PROFILE_MODIFIED: ACL Table profile modified, Save and Reload the device for the profile to be effective | Critical      | The ACL table profile can be modified to increase/decrease the size allocated to a particular application by adjusting the sizes. The profile modification requires a reload. This is specific to the S51xx series of platforms.                         | Reload the device for the modified profile to become effective.   |
| %ACL_LOGGING: ACL_LOG:  | Warning       | When the "log" action is enabled on a user created access-list applied to an interface, the system log message is generated displaying the packet contents which match the access-list rule.   | No action required.   |
| %ACL_LOGGING_FOR_EGRESS_ACL: Logs cannot be generated for Egress ACL  | Warning       | When the "log" action is enabled on a user created access-list applied to an interface in the egress direction, then the system log is generated indicating  | The rule gets programmed in the Egress ACL hardware but the log messages for the  |

**Table 3. OS10 ACL system log messages (continued)**

| <b>System log message</b> | <b>Severity</b> | <b>Description</b>                             | <b>Recommended action</b>             |
|---------------------------|-----------------|--|---------------------------------------|
|                           |                 | that logging cannot be done in the egress ACL. | matching rules will not be displayed. |



## AFS system log message reference

This section lists the messages that are generated by the AFS process.

**Table 4. OS10 AFS system log messages**

| System log message  | Severity      | Description   | Recommended action  |
|---|---------------|---|---|
| %<br>INFRA_AFS:MAC_MOVE_VIOLATION original-ifname<br>ethernet1/1/1,offending-ifname<br>ethernet1/1/2,MAC<br>00:00:00:00:00:10,vlan 10 | Informational | When port security is configured, MAC move violation occurs from secure port eth 1/1/1 to secure port eth 1/1/2, Port security violation.   | Check whether the host movement is valid or not. If host movement is valid, check the port security MAC move configuration. For more information, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/port-security?guid=guid-c27a9d47-ea59-48cc-b19d-90a9f6d52629&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/port-security?guid=guid-c27a9d47-ea59-48cc-b19d-90a9f6d52629&amp;lang=en-us</a> .                               |
| %INFRA_AFS:MAC_LEARN_LIMIT_VIOLATION: ifname<br>ethernet1/1/31,MAC<br>00:00:02:00:0a:05,vlan 1  | Informational | When port security is configured, new MAC 00:00:02:00:0a:05 is trying to get learnt on port eth 1/1/31 after the configured MAC learning limit is reached. Port security violation. | Check whether the maximum number of hosts on that port is valid or not. If the hosts are valid, check the port Security MAC Learning Limit configuration. For more information, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/port-security?guid=guid-c27a9d47-ea59-48cc-b19d-90a9f6d52629&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/port-security?guid=guid-c27a9d47-ea59-48cc-b19d-90a9f6d52629&amp;lang=en-us</a> . |
| )<br>%INFRA_AFS:PVLAN_STATIC_MAC: Duplicate mac<br>00:00:02:00:0a:00 detected on<br>interface ethernet1/1/32, vlan 30                 | Informational | When PVLAN is configured, the MAC address that is statically configured on one secondary VLAN is dynamically learnt or moved to another secondary VLAN of the PVLAN domain.         | Check whether the configured static MAC is valid or not. For more information see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/static-mac-address?guid=guid-a778d001-eef9-4eb9-a4b1-4c02b82ef528&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/static-mac-address?guid=guid-a778d001-eef9-4eb9-a4b1-4c02b82ef528&amp;lang=en-us</a> .   |

# ALM\_ACCNT\_MAC system log message reference

This section lists the system log messages generated by the ALM\_ACCNT\_MAC process.

**Table 5. ALM\_ACCNT\_MAC system log messages**

| System log message                               | Severity      | Description   | Recommended action  |
|--|---------------|---|---------------------|
| %ALM_ACCNT_EVENT:<br>Accounting event was raised | Informational | Information about session details during user login. When AAA accounting is configured, these logs will be seen for each user during login. | No action required. |

# ALM\_CLOCK system log message reference

This section lists the system log messages generated by the ALM\_CLOCK process.

**Table 6. ALM\_CLOCK system log messages**

| System log message               | Severity      | Description   | Recommended action  |
|----------------------------------|---------------|---|---------------------|
| %ALM_CLOCK_UPDATE: Clock changed | Informational | The System clock is changed.<br>ALM_CLOCK_UPDATE: Clock changed | No action required. |

## BFD system log message reference

This section lists the system log messages generated by the BFD process.

**Table 7. BFD system log messages**

| System log message                     | Severity      | Description                                  | Recommended action  |
|--|---------------|--|---------------------|
| %BFD_STATE_CHANGE:<br>Session state to | Informational | Session state has changed for a BFD session. | No action required. |

## BGP system log message reference

This section lists the system log messages that are generated by the BGP process.

**Table 8. BGP system log messages**

| System log message   | Severity      | Description   | Recommended action   |
|--|---------------|---|--|
| %BGP_NBR_NOTIFY_EST_STAT<br>E: BGP FSM established state change Notification | Informational | BGP session successfully established with configured peer. BGP peering successful.  | No action required.  |
| %BGP_NBR_BKWD_STATE_CH<br>G: Backward state change occurred                  | Critical      | Configured BGP session went down. Configured BGP session went down.   | Need to check the connectivity and involve support team.           |
| %BGP_NBR_BKWD_STATE_CH<br>G: Backward state change occurred ADJCHANGE: %s    | Critical      | Connection with BGP neighbor is closed. VRF %s Connection with neighbor over %s closed. 1. "Mem-alloc fail for nbr:%s in VRF %s" 2. "IFM state off nbr %s in VRF %s closed" 3. "TCP FATAL error with nbr %s in VRF %s" 4. "Connection reset by nbr %s in VRF %s" 5. "TCP error with nbr %s in VRF %s" 6. "Connection with nbr %s in VRF %s closed. Fastfallover" 7. "Connection with internal nbr %s in VRF %s closed. Fastfallover" 8. "Hold Time expired for Nbr:%s VRF:%s" NOTE: VRF %s denotes VRF <vrf_name> Nbr:%s denotes Nbr IP or unnumbered peer interface name | Check the connectivity and contact Technical Support, if required. |
| %BGP_NBR_BKWD_STATE_CH<br>G: Backward state change occurred PEER ERR: %s     | Critical      | Connection with BGP neighbor is closed. VRF %s Connection with neighbor over %s closed. 1. "NBR already exists closing con for Nbr:%s VRF:%s" 2. "NBR unconfigured by user for peer :%s VRF:%s" 3. "NBR session reset by user;closed connection for Nbr:%s VRF:%s" 4. "NBR shut by user;closed connection for Nbr:%s VRF:%s" 5. "Neighbor recycled closing connection for Nbr:%s VRF:%s" 6. " Neighbor deleted by user.Connection closed for Nbr:%s VRF:%s" 7. "RR config changed connection recycled for Nbr:%s VRF:%s" 8. "peer   | Check the configuration of peer and involve support team.          |

**Table 8. BGP system log messages (continued)**

| System log message   | Severity | Description  | Recommended action   |
|--|----------|--|--|
|  |          | connectivity lost/fall-over for Nbr over:%s VRF:%s"<br>NOTE: VRF %s denotes VRF <vrf_name> Nbr:%s denotes Nbr IP or unnumbered peer interface name   |  |
| %BGP_NBR_BKWD_STATE_CH<br>G: Backward state change occurred OPEN ERR: %s   | Critical | Connection with BGP neighbor is closed due to error in one of the attributes/options received in OPEN message. VRF %s Connection with neighbor over %s closed. 1. "BAD Version recvd from Nbr over:%s VRF:%s" 2. "BAD AS recvd from Nbr:%s VRF:%s" 3. "BAD HOLD time recvd from Nbr:%s VRF:%s" 4. "BAD BGP ID recvd from Nbr:%s VRF:%s" 5. "Unsupported options recvd from Nbr:%s VRF:%s" 6. "Authentication failure for Nbr:%s VRF:%s" 7. "Bad AFI Cfg from Nbr:%s VRF:%s" 8. "Open Error recvd from Nbr:%s VRF:%s" NOTE: VRF %s denotes VRF <vrf_name> Nbr:%s denotes Nbr IP or unnumbered peer interface name   | Check the connectivity and contact Technical Support, if required.   |
| %BGP_NBR_BKWD_STATE_CH<br>G: Backward state change occurred UPDATE ERR: %s | Critical | Connection with BGP neighbor is closed due to error in one of the attributes in UPDATE message. ADJCHANGE: VRF %s Connection with neighbor over %s closed. 1. "Malformed Attribute rcvd from Nbr over:%s VRF:%s" 2. "UNR well-known attribute rcvd from Nbr over:%s VRF:%s" 3. "missing well-known attribute from Nbr over:%s VRF:%s" 4. "Attribute flag error rcvd from Nbr over:%s VRF:%s" 5. "attribute len err rcvd from Nbr over:%s VRF:%s" 6. "Invalid origin attribute rcvd from Nbr over:%s VRF:%s" 7. "Routing loop detected for Nbr over:%s VRF:%s" 8. "Invalid nexthop rcvd from Nbr over:%s VRF:%s" 9. "optional attribute err rcvd from Nbr over:%s VRF:%s" 10. "Invalid network field rcvd from Nbr over:%s VRF:%s" 11. "Malformed AS_PATH attribute rcvd from Nbr over:%s VRF:%s" 12. | Verify the configuration and correct (if required) the configuration related to error message and if the issue still persists, contact support team. |

**Table 8. BGP system log messages (continued)**

| System log message   | Severity | Description  | Recommended action   |
|--|----------|--|--|
|  |          | "BAD UPD msg rcvd from Nbr over:%s VRF:%s" 13. "Update err rcvd from Nbr over:%s VRF:%s" NOTE: VRF %s denotes VRF <vrf_name> Nbr:%s denotes Nbr IP or unnumbered peer interface name   |  |
| %BGP_NBR_BKWD_STATE_CH G: Backward state change occurred HEADER ERROR:%s | Critical | Connection with BGP neighbor is closed due to error in HEADER of the message received. ADJCHANGE: VRF %s Connection with neighbor over %s closed. 1. "Bad message length from nbr over:%s VRF:%s" 2. "Header not synced. Nbr over:%s VRF:%s" 3. "Bad msg type from Nbr over:%s VRF:%s" 4. "Header err from nbr over:%s VRF:%s" NOTE: VRF %s denotes VRF <vrf_name> Nbr:%s denotes Nbr IP or unnumbered peer interface name   | Contact Support team with the error log.   |
| %BGP_NBR_BKWD_STATE_CH G: Backward state change occurred PGR ERR: %s     | Critical | Connection with BGP neighbor is closed due to Peer group configuration. ADJCHANGE: VRF %s Connection with neighbor over %s closed. 1. "NBR over:%s,VRF:%s removed from peer grp %s" 2. "Peer Group shut connection closed for Nbr over:%s VRF:%s" 3. "Peer Group remote-as removed for Nbr over:%s VRF:%s" 4. "Peer Group deleted for Nbr over:%s VRF:%s" NOTE: VRF %s denotes VRF <vrf_name> Nbr:%s denotes Nbr <IP or unnumbered peer interface name> peer grp %s denotes peer grp <peer-group name> | Verify the configuration related to the error message and correct it if required.  |
| %BGP_NBR_BKWD_STATE_CH G: Backward state change occurred MISC ERR: %s    | Critical | Connection with the BGP neighbor is closed. ADJCHANGE: VRF %s Connection with neighbor over %s closed. 1. "FSM error for Nbr over:%s VRF:%s" 2. "Connection Collision for Nbr over:%s VRF:%s" 3. "Max-Prfx Limit reached for Nbr over:%s VRF:%s" 4. "BGP Session deleted for Nbr over:%s VRF:%s" 5. "Session closed for Nbr over:%s VRF:%s" 6. "Error in Hold Time for Nbr over:%s VRF:%s" 7. "FSM EVT error Nbr:%s VRF:%s"  | Verify the configuration and correct (if required) the configuration related to error message and if the issue still persists, contact support team. |

**Table 8. BGP system log messages (continued)**

| System log message  | Severity      | Description  | Recommended action  |
|---|---------------|--|---|
|   |               | 8. "Router-id changed Nbr over:%s VRF:%s recycled" 9. "Invalid martian next hop for Nbr over:%s VRF:%s" 10. "Attribute len error for Nbr over:%s VRF:%s" 11."BFD Nbr over:%s VRF:%s DOWN" 12. "ADDPATH Denied Nbr over:%s VRF:%s" NOTE: VRF %s denotes VRF <vrf_name> Nbr:%s denotes Nbr <IP or unnumbered peer interface name>  |   |
| %BGP_MAX_PRFX_REACHED: Maximum prefix limit per peer exceeded.            | Critical      | The number of prefixes sent to this BGP neighbor or peer reached the threshold value (a percentage of the maximum number of prefixes allowed). "Max Prefix hit from nbr:%s in VRF:%s" NOTE: VRF %s denotes VRF <vrf_name> Nbr:%s denotes Nbr <IP or unnumbered peer interface name>  | Use the neighbor maximum-prefix command to change the threshold value for that BGP neighbor or peer.  |
| %BGP_MAX_PRFX_THRESHOLD: Maximum prefix threshold limit per peer reached. | Warning       | The number of route prefixes sent to a BGP neighbor exceeds the number allowed in its configuration. "Max Prefix Threshold hit from nbr:%s in VRF:%s" NOTE: VRF %s denotes VRF <vrf_name> Nbr:%s denotes Nbr <IP or unnumbered peer interface name>  | Determine if the neighbor is configured properly. Use the neighbor maximum-prefix command to increase the number of prefixes allowed for that BGP neighbor or peer. |
| %BGP_RM_OPER_STATE_CHANGE: RM operational state is changed.               | Informational | BGP process operational status is changed. "Received RM State Change trap RM(vrf) %s Oper_status:%d" NOTE: VRF %s denotes VRF <vrf_name> Oper_status:%d denotes Oper_status 1(UP) or 2(DOWN) or 3(GOING UP) or 4(GOING DOWN) or 5(FAILED).   | No Action required.   |
| %BGP_NOTIFY_CONFIG_ERROR: Config Error                                    | Warning       | BGP configuration failed due to mentioned reason. Config Error %S 1. PGR <pgr-name> with add-path configured when peer list has unnumbered neighbor.2. suppress-map will override summary-only option 3. "Attempt to configure Passive peergroup when peer list has unnumbered neighbor." 4. "PGR and PEER Area Mismatch.Config NotAllowed" 5. "Password configuration failed" 6. "Unnum PGR remote as configured when | Refer to the configuration guidelines. If the issue persists, contact Technical Support.  |



**Table 8. BGP system log messages (continued)**

| System log message  | Severity      | Description   | Recommended action  |
|---|---------------|---|---------------------|
|   |               | peer list has unnumbered neighbor." 7. "PGR and PEER Area Mismatch Config " 8. "Unnum PGR with ebgp-multihop configured when peer list has unnumbered neighbor." 9. "Unnum PGR with fallover configured when peer list has unnumbered neighbor." 10. "Unnum PGR with route-reflector-client configured when peer list has unnumbered neighbor." 11. "Unnum PGR with update-source configured when peer list has unnumbered neighbor." NOTE: %S denotes the configuration error resulted |                     |
| %ROUTE_MAP_MATCH_PARAM  | Informational | Route-map <rmap-name>: Match address based on ACL is not applicable for Routing modules in VRF <vrf-name>.  | No Action required. |
| IPv6 Extended Prefix support not configured   | Informational | Unable to program routes with prefix length > 64 and < 128.   | No Action required. |
| %UNNUMBERED_NEXT_HOP: Clear all BGP unnumbered sessions for Nexthop to be global unicast followed by link-local address | Informational | When the BGP unnumbered feature is disabled globally at ROUTER BGP level, a System log message is displayed, recommending you to reset all unnumbered peers to restore to legacy behavior.  | No Action required. |
| %UNNUMBERED_NEXT_HOP: Link-local nexthop configuration in peer-group pg1 is applicable only for unnumbered peers        | Informational | When link-local-only-nexthop is configured in a template with at least one IP peer, a System log message is displayed, notifying that the configuration is applicable for unnumbered peers only.  | No Action required. |
| %UNNUMBERED_NEXT_HOP: Link-local nexthop configuration in peer-group pg1 is applicable only for unnumbered peers        | Informational | When template with link-local-only-nexthop configured is being inherited to an IP peer, a System log message is displayed stating that the configuration is applicable only on unnumbered peers.  | No Action required. |

## CMS system log message reference

This section lists the system log messages that the CMS process generates.

**Table 9. CMS system log messages**

| System log message          | Severity      | Description  | Recommended action   |
|-----------------------------|---------------|--|--|
| %CMS_INIT_STATE: init state | Informational | The log indicates the new state, the CMS module is transitioning to. On system boot, the CMS should eventually transition to state 6. Transitioning to state 6 indicates successful initialization of the CMS module. System log message specifies that the current state - the CMS module - is transitioning information. | On startup, if the system does not transition to state 6, the CMS module could be applying the startup configuration. If the state persists for a long period, contact Technical Support for further assistance. |

# Configuring LLFC system log message reference

This section lists the system log message for configuring LLFC on discovery ports from OS10 release 10.5.2.3.

**Table 10. Configuring LLFC**

| System log message   | Severity      | Description   | Recommended action  |
|--|---------------|---|---------------------|
| LLFC_ON_ICL_DISCOVERY_PORT : LLFC enabled on ICL discovery port <interface name> | Informational | This system log message is generated when the user configures LLFC on discovery ports and vice-versa. | No action required. |

## DCBX system log messages

This section lists the system log messages that the DCBX process generates.

**Table 11. DCBX system log messages**

| System log message  | Severity      | Description   | Recommended action   |
|---|---------------|---|--|
| %DCBX_PFC_PORT_OPER_UP: PFC Parameters MATCH on interface           | Informational | PFC configuration of remote port matches local PFC configuration.         | No action required.  |
| %DCBX_PFC_PORT_OPER_DOWN: PFC Parameters MISMATCH on interface      | Informational | PFC configuration of remote port does not match local PFC configuration.  | Check local and remote PFC configuration.  |
| %DCBX_ETS_PORT_OPER_UP: ETS Parameters MATCH on interface           | Informational | ETS configuration of the remote port matches the local ETS configuration. | No Action Required.  |
| %DCBX_ETS_PORT_OPER_DOWN: ETS Parameters MISMATCH on interface      | Informational | ETS configuration of remote port does not match local ETS configuration.  | Check local and remote ETS configurations.   |
| %DCBX_PEER_ETS_STATE_CHANGE: ETS Peer state change                  | Informational | When there is a change in ETS state. (enable or disable)                  | No action required.  |
| %DCBX_PEER_PFC_STATE_CHANGE: PFC Peer state change                  | Informational | When there is change in PFC state. (enable or disable)                    | No action required.  |
| %DCBX_PEER_VER_CONFLICT: DCBX Peer version conflict on              | Informational | Remote port has different version of DCBX.                                | Check the version of DCBX on local and remote port.                                  |
| %DCBX_UNRECOGNIZED_TLV: Received Unrecognized DCBX TLV              | Informational | DCBX TLV is not recognized.   | Contact technical support for further assistance.                                    |
| %DCBX_PFC_MAX_CAP_EXCEEDED: Peer PFC Capability exceeded max limit. | Warning       | PFC enabled priorities are greater than maximum supported.                | Contact your technical support for further assistance on the local and remote ports. |
| %DCBX_ETS_RECV_CONFIG_ERROR: Peer ETS config error                  | Warning       | Indicates that there is an error in the remote ETS configuration.         | Check the remote port ETS configuration. Contact Technical Support for assistance.   |

## DENIED\_ARP system log message reference

This section lists the system log messages that are generated by the DENIED\_ARP process.

**Table 12. DENIED\_ARP system log messages**

| System log message                           | Severity      | Description  | Recommended action  |
|--|---------------|--|---------------------|
| %DENIED_ARP_PACKET:<br>DAI:Denied ARP packet | Informational | The ARP packets denied by Dynamic ARP inspection as this ARP packet does not match the DAI rules and dropped. Dynamic ARP Inspection feature will check source IP, source mac , interface and VLAN of the ARP packets and forward the ARP packets only if it is present in the list of allowed entries (DAI database). If it is not present in the list of allowed entries, then the ARP packets will be dropped by default. The DAI database is updated with the learned entries, when a new entry learned and added in the DHCP snooping database. | No action required. |

## DOT1X system log message reference

This section lists the system log messages that are generated by the DOT1X process.

**Table 13. DOT1X system log messages**

| System log message                                      | Severity      | Description                                       | Recommended action   |
|---|---------------|---|--|
| %DOT1X_PDU_TX_FAIL: PDU Transmission Failed             | Informational | PDU Transmission Failed.                          | If the message is displayed document the message exactly as it appears and contact your technical support representative for assistance. |
| %DOT1X_PDU_RX_FAIL: PDU Reception Failed                | Informational | Dot1x PDU reception failed. PDU Reception Failed. | If the message is displayed document the message exactly as it appears and contact your technical support representative for assistance. |
| %DOT1X_ACL_INSTALL_FAIL: ACL filter installation failed | Informational | ACL filter installation failed.                   | If the message is displayed document the message exactly as it appears and contact your technical support representative for assistance. |

## DYNAMIC\_MGMT system log message reference

This section lists the system log messages that are generated by the DYNAMIC\_MGMT process.

**Table 14. DYNAMIC\_MGMT system log messages**

| System log message  | Severity      | Description  | Recommended action  |
|---|---------------|--|---------------------|
| %DYNAMIC_MGMT_ROUTE_OVERRIDEWRITE: Overriding route obtained via DHCP/Autoconf with static route. | Informational | Route configured is overridden by route via DHCP/AutoConf. | No action required. |

## EQM system log message reference

This section lists the system log messages that are generated by the EQM process.

**Table 15. EQM system log messages**

| System log message                                       | Severity      | Description   | Recommended action  |
|--|---------------|---|---|
| %EQM_UNIT_UP: Unit is up                                 | Informational | Equipment Manager declared the card is ready.   | No action required.   |
| %EQM_UNIT_DOWN: Unit is down                             | Critical      | Equipment Manager detected the card is reset.   | No action required.   |
| %EQM_UNIT_PWRON: Unit powered-on                         | Informational | Equipment Manager detected the card is powered on and it is in the process of check-in. | No action required.   |
| %EQM_UNIT_RESET: Unit is being reset                     | Informational | Equipment Manager detected the card is checked-in after reset.                          | No action required.   |
| %EQM_UNIT_DETECTED: Unit present                         | Informational | Equipment Manager detected the card.  | No action required.   |
| %EQM_UNIT_CHECKIN: Unit check-in detected                | Informational | Equipment Manager identified the specific card-type and the system ports.               | No action required.   |
| %EQM_UNIT_RETRY_RESET: Unit power cycled reload          | Informational | Equipment Manager retrying reset due to some problem detected.                          | No action required.   |
| %EQM_UNIT_SHUTDOWN: Unit shut down                       | Critical      | Equipment Manager forcing shutdown on the card due to some problem.                     | Check for other alarms related to temperature etc.  |
| %EQM_UNIT_NO_CHECKIN: Unit not check-in                  | Warning       | Equipment Manager does not detect the card checked-in.                                  | Check for any service failures in the system.   |
| %EQM_SYSTEM_RELOAD: User request to reload system        | Informational | Reboot has been initiated by user.  | No action required.   |
| %EQM_PSU_DETECTED: Power supply unit present             | Informational | PSU has been detected.  | No action required.   |
| %EQM_PSU_OFF: Power supply unit power off or removed     | Critical      | PSU has been removed or power has been turned off for the PSU.                          | If not expected, check the PSU and the power-source for any loose contacts, or loss of power.       |
| %EQM_FAN_TRAY_DETECTED: Fan tray present                 | Informational | Fan Tray has be detected.   | No action required.   |
| %EQM_FAN_TRAY_OFF: Fan tray power off or removed         | Critical      | Fan tray has been removed.  | If not expected, check for any loose contacts or device not being seated properly.                  |
| %EQM_PAS_NOT_READY: PAS service is not ready             | Critical      | PAS service has not yet come up.  | Check if PAS has crashed. Typically system will reboot after some time.                             |
| %EQM_TML_WARN_CROSSED: Thermal threshold crossed warning | Warning       | One of the temperature sensors has crossed the "Warning Threshold".                     | Check the environment, any fan trays being faulty etc. The fans speeds will increase automatically. |



**Table 15. EQM system log messages (continued)**

| System log message  | Severity      | Description  | Recommended action  |
|---|---------------|--|---|
| %EQM_TML_MINOR_CROSSED : Thermal threshold crossed minor warning  | Warning       | One of the temperature sensors has crossed the "Minor Threshold".                | Check the environment, for example, faulty fan tray, and fix them. The fans speeds will increase automatically. |
| %EQM_TML_MAJOR_CROSSED : Thermal threshold crossed major warning  | Critical      | One of the temperature sensors has crossed the "Minor Threshold".                | Check the environment, any fan trays being faulty etc. The fans speeds will increase automatically.             |
| %EQM_TML_CRIT_CROSSED: Thermal threshold crossed critical warning | Critical      | One of the temperature sensors has crossed the "Critical Threshold".             | Check the environment, any fan trays being faulty etc. The fans speeds will increase automatically.             |
| %EQM_FAN_FAULT_MINOR: Fan fault minor warning                     | Warning       | One of the Fan is malfunctioning.  | remove and reinsert the corresponding fantray.  |
| %EQM_FAN_FAULT_MAJOR: Fan tray fault major warning                | Critical      | A major fault is present with one of the fan tray.                               | remove and reinsert the corresponding fantray.  |
| %EQM_FANTRAY_FAULT: Fan tray fault                                | Warning       | A fant-tray is faulty.   | remove and reinsert the corresponding fantray.  |
| %EQM_FANTRAY_NOT_PRESENT: Fan tray absent                         | Warning       | A fan tray is removed or not detected.   | If you you feel this is a false alarm, remove and re-insert the fan tray.                                       |
| %EQM_PSU_FAULT: Power supply unit (PSU) fault                     | Warning       | PSU is faulty.   | Check if PSU and power-cable is properly inserted. Check if the power-source is working properly.               |
| %EQM_PSU_NOT_PRESENT: Power supply unit (PSU) absent              | Warning       | PSU has been removed.  | If this is not expected, check if the PSU is properly inserted.   |
| %EQM_MORE_PSU_ABSENT: More power supply unit (PSU) absent         | Critical      | If the platform has many PSU slots this indicates absence of multiple PSU units. | If this is not expected, check if the PSU is properly inserted.   |
| %EQM_MORE_PSU_FAULT: More power supply unit (PSU) fault           | Critical      | IF the PSU has multiple PSU faults.  | Check if PSU and power-cable is properly inserted. Check if the power-source is working properly.               |
| %EQM_PSU_FAULT_CRIT: Power supply unit (PSU) fault alert          | Critical      | Power Source has failed.   | Check power-source.   |
| %EQM_FAN_AIRFLOW_UNKNOWN: Fan airflow speed unknown               | Warning       | If the airflow direction cannot be determined.                                   | Check if device is properly inserted.   |
| %EQM_FAN_AIRFLOW_MISMATCH: Fan airflow speed mismatch             | Critical      | If fan trays are not mutually compatible.  | Check the PPID of all fan trays or PSU for compatible.  |
| %EQM_ALL_FANTRAY_ABSENT : All fan trays absent                    | Critical      | If none of the fan trays are inserted.   | If fan trays are inserted check that they are seated properly.  |
| %EQM_ALL_FANTRAY_FAULT: All fan trays fault                       | Critical      | If all fan trays are faulty.   | If fan trays are inserted check whether they are seated properly, and there is no blockage in air circulation.  |
| %EQM_MEDIA_PRESENT: Media inserted                                | Informational | A media(port) is inserted.   | No action required.   |

**Table 15. EQM system log messages (continued)**

| <b>System log message</b>  | <b>Severity</b> | <b>Description</b>   | <b>Recommended action</b>  |
|--|-----------------|--|--|
| %EQM_MEDIA_NOT_PRESENT: Media removed  | Critical        | A media(port) is removed.  | If not expected, check whether the media is properly inserted.   |
| %EQM_MEDIA_QSA28_EXPECTED: QSA28 adapter expected  | Critical        | The platform expects a QSA28 adapter, but the inserted optics is not QSA28.              | Check the media adapter connected to the port. If the media adapter is a QSA adapter, then replace the adapter with a QSA28 adapter. |
| %EQM_VERSION_MISMATCH: Unit down reason: version mismatch                                    | Informational   | Unit went down due to version mismatch.  | No action required.  |
| %EQM_TYPE_MISMATCH: Unit down reason: type mismatch  | Informational   | Unit went down due to equipment type mismatch.   | No action required.  |
| %EQM_ADMIN_DOWN: Unit down reason: admin down  | Informational   | Unit went down due to admin state down.  | No action required.  |
| %EQM_UNLICENSED: Unit down reason: unlicensed  | Informational   | Unit went down due to unlicensed reason.   | No action required.  |
| %EQM_SOFTWARE_TRIGGERED: Unit down reason: software triggered                                | Informational   | Unit went down due to software triggered reset.  | No action required.  |
| %EQM_UNIT_CRASHED: Unit down reason: unit crashed  | Informational   | Unit went down due to unit crash.  | No action required.  |
| %EQM_UNKNOWN: Unit down reason: unknown  | Informational   | Unit went down due to unknown reason.  | No action required.  |
| %EQM_LPC_FAULT: LPC bus error  | Critical        | Fault detected due to LPC bus error.   | Contact support team for RMA process.  |
| %EQM_MEDIA_TEMP_HIGH: Media high temperature threshold crossed major warning                 | Critical        | Digital Optical Monitoring detects that the high temperature major threshold is crossed. | Check fan units and check whether the media type is supported. Try replacing the media.  |
| %EQM_MEDIA_TEMP_HIGH_WARNING: Media high warning temperature threshold crossed minor warning | Warning         | Digital Optical Monitoring detects that the high temperature minor threshold is crossed. | Check fan units and check whether the media type is supported. Try replacing the media.  |
| %EQM_MEDIA_TEMP_LOW_WARNING: Media low warning temperature threshold crossed minor warning   | Warning         | Digital Optical Monitoring detects that the low temperature minor threshold is crossed.  | Check fan units and check whether the media type is supported. Try replacing the media.  |
| %EQM_MEDIA_TEMP_LOW: Media low temperature threshold crossed major warning                   | Critical        | Digital Optical Monitoring detects that the low temperature major threshold is crossed.  | Check fan units and check whether the media type is supported. Try replacing the media.  |
| %EQM_MEDIA_VOLTAGE_HIGH: Media high voltage threshold crossed major warning                  | Critical        | Digital Optical Monitoring detects that the high voltage major threshold is crossed.     | Check fan units and check whether the media type is supported.. Try replacing the media.   |
| %EQM_MEDIA_VOLTAGE_HIGH_WARNING: Media high warning voltage threshold crossed minor warning  | Warning         | Digital Optical Monitoring detects that the high voltage minor threshold is crossed.     | Check whether the media is supported. Try replacing the media.   |

**Table 15. EQM system log messages (continued)**

| <b>System log message</b>   | <b>Severity</b> | <b>Description</b>  | <b>Recommended action</b>                                      |
|---|-----------------|---|--|
| %EQM_MEDIA_VOLTAGE_LOW_WARNING: Media low warning voltage threshold crossed minor warning     | Warning         | Digital Optical Monitoring detects that the low voltage minor threshold is crossed.       | Check whether the media is supported. Try replacing the media. |
| %EQM_MEDIA_VOLTAGE_LOW: Media low voltage threshold crossed major warning                     | Critical        | Digital Optical Monitoring detects that the low voltage major threshold is crossed.       | Check whether the media is supported. Try replacing the media. |
| %EQM_MEDIA_RX_POWER_HIGH: Media high rx_power threshold crossed major warning                 | Critical        | Digital Optical Monitoring detects that the high rx power major threshold is crossed.     | Check whether the media is supported. Try replacing the media. |
| %EQM_MEDIA_RX_POWER_HIGH_WARNING: Media high warning rx_power threshold crossed minor warning | Warning         | Digital Optical Monitoring detects that the high rx power minor threshold is crossed.     | Check whether the media is supported. Try replacing the media. |
| %EQM_MEDIA_RX_POWER_LOW_WARNING: Media low warning rx_power threshold crossed minor warning   | Warning         | Digital Optical Monitoring detects that the low rx power minor threshold is crossed.      | Check whether the media is supported. Try replacing the media. |
| %EQM_MEDIA_RX_POWER_LOW: Media low rx_power threshold crossed major warning                   | Critical        | Digital Optical Monitoring detects that the low rx power major threshold is crossed.      | Check whether media is supported. Try replacing the media.     |
| %EQM_MEDIA_TX_POWER_HIGH: Media high tx_power threshold crossed major warning                 | Critical        | Digital Optical Monitoring detects that the high tx power major threshold is crossed.     | Check whether the media is supported. Try replacing the media. |
| %EQM_MEDIA_TX_POWER_HIGH_WARNING: Media high warning tx_power threshold crossed minor warning | Warning         | Digital Optical Monitoring detects that the high tx power minor threshold is crossed.     | Check whether the media is supported. Try replacing the media. |
| %EQM_MEDIA_TX_POWER_LOW_WARNING: Media low warning tx_power threshold crossed minor warning   | Warning         | Digital Optical Monitoring detects that the low tx power minor threshold is crossed.      | Check whether the media is supported. Try replacing the media. |
| %EQM_MEDIA_TX_POWER_LOW: Media low tx_power threshold crossed major warning                   | Critical        | Digital Optical Monitoring detects that the low tx power major threshold is crossed.      | Check whether the media is supported. Try replacing the media. |
| %EQM_MEDIA_BIAS_HIGH: Media high bias threshold crossed major warning                         | Critical        | Digital Optical Monitoring detects that the high bias current major threshold is crossed. | Check whether the media is supported. Try replacing the media. |
| %EQM_MEDIA_BIAS_HIGH_WARNING: Media high warning bias threshold crossed minor warning         | Warning         | Digital Optical Monitoring detects that the high bias current minor threshold is crossed. | Check whether the media is supported. Try replacing the media. |
| %EQM_MEDIA_BIAS_LOW_WARNING: Media low warning bias threshold crossed minor warning           | Warning         | Digital Optical Monitoring detects that the low bias current minor threshold is crossed.  | Check whether media is supported. Try replacing the media.     |
| %EQM_MEDIA_BIAS_LOW: Media low bias threshold crossed major warning                           | Critical        | Digital Optical Monitoring detects that the low bias current major threshold is crossed.  | Check whether media is supported. Try replacing the media.     |

## ETL system log message reference

This section lists the system log messages that are generated by the ETL process.

**Table 16. ETL system log messages**

| System log message   | Severity      | Description   | Recommended action   |
|--|---------------|---|--|
| %ETL_SERVICE_UP: ETL service is up   | Informational | Event Logger Service is up. ETL service is up.  | No action required.  |
| %ETL_HOST_UNREACHABLE: Destination host unreachable                          | Informational | Logging Server is unreachable. Destination host unreachable.  | Check logging server connectivity to the system.   |
| %ETL_RELOAD_CFG_FAIL: OS10 system log manager unable to reload configuration | Warning       | An error occurred while restarting the syslog service with the configuration. OS10 system log manager unable to reload configuration. | Save the log file and any debug messages and contact your technical support representative for further analysis. |

## EVPN system log message reference

This section lists the system log messages that are generated by the EVPN process.

**Table 17. EVPN system log messages**

| System log message               | Severity      | Description  | Recommended action   |
|----------------------------------|---------------|--|--|
| %EVPN_MAC_ERROR: EVPN MAC error: | Informational | System detects 5 mac station move between VTEPs with in 3 min. EVPN MAC %s error %s for MAC %s | Without any user action, VMs move between VTEPs, check for any duplicate MACs present in the VMs. For more information, refer to the VXLAN and BGP EVPN Configuration Guide for Dell SmartFabric OS10 Release 10.5.2.. |

# FC\_SVCS system log message reference

This section lists the system log messages that are generated by the FC\_SVCS process.

**Table 18. FC\_SVCS system log messages**

| System log message   | Severity      | Description  | Recommended action  |
|--|---------------|--|---|
| %FC_SVCS_MS_START_FABRIC_RECONFIG: The Switch Starts                                 | Informational | This log is displayed in Multi-switch mode, where any link failure in the fabric that may result in Build Fabric operation causing the Principal switch re-election.   | <ul style="list-style-type: none"> <li>Check if any node has left the fabric due to link failure.</li> <li>Check if any configured fabric joins with another fabric.</li> <li>Check is there any domain ID overlap when joining configured fabric with another configured fabric in case of RCF.</li> </ul> |
| %FC_SVCS_MS_START_PRNCPL_ELECTION: The Switch Starts Principal Switch Election       | Informational | This log is displayed whenever the Principal switch election happens in the switch.  | No action required.   |
| %FC_SVCS_MS_PRNCPL_ELECTION_CMPLTD: Principal Switch Election Completed.             | Informational | This log is displayed after Principal switch election is completed.  | No action required.   |
| %FC_SVCS_MS_DOMAINID_ASIGN: DomainID   | Informational | This log is no longer valid.   | This log is no longer valid.  |
| %FC_SVCS_MS_NOT_CAPABLE_PRNCPL_SWITCH: No Switch Capable to Become Principal Switch. | Informational | This log is displayed when the principal-priority on a switch is set to 255.   | If user wants want this switch to become principal switch, then change the principal-priority value accordingly in vfabric configuration.   |
| %FC_SVCS_MS_STABLE: The Switch reaches the Stable State                              | Informational | This log is displayed after Principal switch election is completed and the switch reaches stable state.  | Information to the user.  |
| %FC_SVCS_MS_EPORT_ISOLATED: Isolated   | Informational | This log is displayed when there is mismatch in timer configuration between two nodes.   | Verify E_D_TOV and R_A_TOV timer configuration on the affected switches.  |
| %FC_SVCS_NPG_SLB_IN_PROGRESS: Re-balance   | Informational | This log is displayed when the user executes the re-balance npg sessions second time where the re-balance is already in progress, i.e user has executed the command again before it completes its operation of 1st executed command. | Wait for the re-balance to complete successfully.   |
| %FC_SVCS_NPG_SLB_SUCCESS: Re-balance   | Informational | This log is displayed after the session re-balance is successful.  | No action required.   |
| %FC_SVCS_NPG_SLB_SUCCESS_STATE_CHANGE: Re-balance                                    | Informational | when a user executes the re-balance npg session, it computes the session distribution. Based on the computation it starts tearing down the session, also 30 second timer starts. The   | User has to execute the re-balance npg sessions again to get the system into balanced state.  |

**Table 18. FC\_SVCS system log messages (continued)**

| System log message                                      | Severity      | Description   | Recommended action  |
|---|---------------|---|---|
|   |               | teared down sessions get logged in successfully within the 30 second time period. After that if there is any state change deducted like enode logged out or uplink going down then this log is raised.  |   |
| %FC_SVCS_NPG_SLB_NOT_SUCCESS: Re-balance                | Informational | This log is raised when the operations got timed-out (30 seconds) for the Vfabric-ID. i.e the sessions did not re-login.  | Try executing the re-balance npg sessions again if issue still persists, shut/no shut the enode ports.  |
| %FC_SVCS_NPG_SLB_NOT_SUCCESS_STATE_CHANGE: Re-balance   | Informational | when a user executes the re-balance npg session, it computes the session distribution. Based on the computation it starts tearing down the session, also 30 second timer starts. The teared down sessions not logged in back and a state change like enode port down, uplink port down or uplink port added then this log will be raised. | Execute the re-balance npg sessions again to get the system into balanced state.  |
| %FC_SVCS_MS_CLASSF_ZERO_CREDIT_TIMEOUT: CLASS-F:        | Informational | This log is displayed when credit for selected CLASS-F frames becomes zero and does not recover for 10 seconds.   | This is the info to customer and Auto recovery in place.  |
| %FC_SVCS_MS_CLASSF_ACK1_TIMEOUT: CLASS-F:               | Informational | This log is displayed if ACK1 is not received from destination domain for 1 second.   | This is the info to customer and Auto recovery in place.  |
| %FC_SVCS_MS_CLASSF_WAIT_TIMEOUT: CLASS-F:               | Informational | This log is displayed when we are about to send frame to destination domain but credit is 0 for 10 second.  | This is the info to customer and Auto recovery in place.  |
| %FC_SVCS_MS_FSPF_FSM: FSPF:                             | Informational | This log is displayed with port id and vfabric id when domain id allocated and FSPF reaches FULL state.   | No action required.   |
| %FC_SVCS_ERR_POOL_MALLOC_FAIL: Memory allocation failed | Critical      | System is out of memory.  | Check the memory usage. Verify the switch configurations are done within the recommended limits Report to customer-support if issue not resolved. |
| %FC_SVCS_FC_FABRIC_UPDATE: Update                       | Informational | This log is displayed when there is an N_port logged in or logged out to the F port device.   | No action required.   |

## FCOE system log message reference

This section lists the system log messages that are generated by the FCOE process.

**Table 19. FCOE system log messages**

| System log message  | Severity      | Description  | Recommended action   |
|---|---------------|--|--|
| %FCOE_RECV_PACKET_ERROR<br>: Packet Receive Error   | Critical      | This error message appears when the FCOE application deletes the FIP deny ACL rule during port transitioning to Operation Up state. If an FIP packet is received during this time, it is dropped.                  | The FCOE session will be formed without any user action, else Shut/ No shut the enode interface.   |
| %FCOE_MAX_VLAN_LIMIT_RCH:<br>H: Number of FIP Snooping enabled VLANs reached maximum allowed limit  | Critical      | The maximum number of vlan on which fip-snooping can be enabled is 12. This log is raised when the limit is reached.   | User has to disable fip-snooping on existing vlan in order to configure to new FCOE VLAN.  |
| %FCOE_MAX_FCF_LIMIT_RCH:<br>Number of FCFs reached maximum allowed limit in VLAN                    | Informational | Maximum number of FCF per VLAN has reached the allowed limit, that is, 12.   | If user wants to add new FCF, then existing FCF has to be removed.   |
| %FCOE_MAX_SESSION_LIMIT_RCH:<br>Number of sessions reached maximum allowed limit for the ENode      | Informational | Maximum session for the enode limit is reached. By default, the number of FCOE sessions is 32. You can increase this limit to 64 by modifying the configuration. The maximum sessions allowed per enode MAC is 64. | 1) If default value is set , then modify the configuration using below command <code>fcoe max-sessions-per-enodemac &lt;1-64&gt;</code> 2) If more than 64 session is required, then add extra enode port as required. |
| %FCOE_FCF_DROP: New FCF discovered in VLAN is dropped as max-FCF-limit per VLAN is reached          | Informational | Maximum number for FCF allowed per vlan is 12. Beyond that it will be dropped.   | If user wants to add new FCF, then existing FCF has to be removed.   |
| %FCOE_ENODE_DROP: New ENode discovered in interface dropped as max-ENode-limit in interface reached | Informational | In FIP snooping bridge mode an enode port allows only one enode. If you want more than one enode to setup a session through the same port, you must move one enode to enode-transit port role.                     | 1) If default value is set , then modify the configuration using below command <code>fcoe max-sessions-per-enodemac &lt;1-64&gt;</code> 2) If more than 64 session is required, then add extra enode port as required. |
| %FCOE_SESSION_DROP: New session request in interface dropped as max-session-limit in enode reached  | Informational | If the configured maximum sessions per enode mac value is reached and any further new session will be dropped.   | 1) If default value is set , then modify the configuration using below command <code>fcoe max-sessions-per-enodemac &lt;1-64&gt;</code> 2) If more than 64 session is required, then add extra enode port as required. |
| %FCOE_CONFLICT_FC_MAP:<br>FIP Snooping conflict in FC MAP for VLAN                                  | Critical      | This log is displayed when the configured FC-MAP value in VLAN Fip-Snooping Bridge is different from the FC-MAP value in F-port.   | Configure same FC-MAP in vlan of Fip Snooping bridge and vfabric in F-port Switch.   |



**Table 19. FCOE system log messages (continued)**

| System log message  | Severity      | Description  | Recommended action   |
|---|---------------|--|--|
| %FCOE_CONFLICT_VLAN: FIP Snooping conflict in FCF advertised VLAN. FIP snooping not enabled for this VLAN   | Critical      | FCOE VLAN is different from the FCF advertised VLAN.   | Configure same FCOE VLAN on all the switches, that is, FSB or NPG and F-port.  |
| %FCOE_SESSION_UPDATE: FCoE Session  | Informational | This log is displayed when a new FCOE session is created or an existing FCOE session is cleared.   | Just an Information to the user.   |
| %FCOE_ENODE_TIMEOUT: FCoE ENode Timeout   | Critical      | This log is displayed where there is no enode keepalive for 5 * FKA advertised by the FCF.   | Check the FCOE client. Try shut or no shut of the enode port. Check VLAN request response is sent.   |
| %FCOE_FCF_TIMEOUT: FCoE FCF Timeout   | Critical      | This log is displayed when there is no FCF advertisement for 5 * FKA_ADV_PERIOD.   | Do shut or no shut of FCF facing port. Check FCOE statistics to verify Multicast FCF advertisement counter is incremented.                 |
| %FCOE_SESSION_TIMEOUT: FCoE Session Timeout   | Critical      | This log is displayed when there is no VN keep alive received from a fcoe client for 5 * FKA_VN_PERIOD (90) seconds.   | After the session time out, the C N A will try to re-establish the session by sending vlan request. If not try shut/no shut of enode port. |
| %FCOE_ENODE_SESSION_LIMIT_CHANGE: One or more ENode MACs have more sessions than the newly configured limit. The new limit will be applied to future sessions | Informational | This log is displayed when we change the value of fcoe max-sessions-per-enodemac. For example their exist 32 sessions and we limit it by setting the value to 10. Existing session will not be affected by this configuration change. But the new session request will be dropped. | Information to the user on configuration change.   |
| %FCOE_APP_TLV: FCOE_APP_TLV   | Informational | This log is displayed when FCOE application TLV is configured.   | No action required.  |

## FEFD system log message reference

This section lists the system log messages that are generated by the FEFD process.

**Table 20. FEFD system log messages**

| System log message   | Severity      | Description   | Recommended action   |
|--|---------------|---|--|
| %FEFD_OUT_OF_MEM: FEFD:<br>Out of Memory   | Informational | The system is running out of memory.<br>System is out of memory.  | Reduce processes if possible.<br>Contact your technical<br>support representative for<br>further analysis. |
| %FEFD_ERROR_SET: Interface<br>set to FEFD Error :  | Informational | This error is set when FEFD port<br>is unable to detect neighbor FEFD<br>peer after 3* interval time configured.<br>Interface set to FEFD Error:  | Enable FEFD on the peer<br>node port.  |
| %FEFD_ERROR_CLR: Interface<br>cleared from FEFD Error :                                    | Informational | If the FEFD port is set<br>to FEFD_ERROR_SET and FEFD<br>configuration is removed, then this<br>indicates that the error set previously<br>was removed. Interface cleared from<br>FEFD error. | No action required.  |
| %FEFD_PORT_BIDIRECTION_DE<br>TECTED: Interface has Bi-<br>directional link with its peer : | Informational | This is informational log to show if<br>FEFD peer is detected. Interface has<br>Bi-directional link with its peer :   | No action required.  |

## IGMP system log message reference

This section lists the system log messages that are generated by the IGMP process.

**Table 21. IGMP system log messages**

| System log message  | Severity      | Description  | Recommended action  |
|---|---------------|--|---------------------|
| %IGMP_SNOOPING_INTERFACE : IGMP Snooping  | Informational | IGMP snooping is configured on a default VLAN, hence it is operationally disabled.<br>IGMP_SNOOPING_INTERFACE: IGMP Snooping disabled on interface :%s | No action required. |
| IGMP or MLD Snooping instance limit exceeded. IGMP or MLD snooping would not be enabled on further VLANs. | Informational | IGMP or MLD Snooping instance limit receded. IGMP or MLD snooping can be enabled on some VLANs.  | No action required. |
| IGMP or MLD Snooping instance limit has receded.  | Informational | You can enable IGMP or MLD Snooping on some VLANs.   | No action required. |

## IP system log message reference

This section lists the system log messages that are generated by the IP system process.

**Table 22. IP system log messages**

| System log message                                | Severity      | Description          | Recommended action  |
|---|---------------|----------------------|---------------------|
| %IP_ADDRESS_ADD: IP Address add is successful.    | Informational | IP Address Addition. | No action required. |
| %IP_ADDRESS_DEL: IP Address delete is successful. | Informational | IP Address Deletion. | No action required. |

## IPv6 system log message reference

This section lists the system log messages that are generated by the IPv6 process.

**Table 23. IPv6 system log messages**

| System log message   | Severity      | Description  | Recommended action  |
|--|---------------|--|---|
| IPv6 Extended Prefix support not configured  | Informational | Unable to program routes with prefix length > 64 and < 128.  | Configure IPv6-extended support and hardware Layer3 IPv6-extended-prefix and reboot the system. You must configure these settings globally. For more information on configuring IPv6-extended prefix, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/hardware-l3-ipv6-extended-prefix?guid=guid-889ed6e9-9728-49e4-9a7c-d35f80663188&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/hardware-l3-ipv6-extended-prefix?guid=guid-889ed6e9-9728-49e4-9a7c-d35f80663188&amp;lang=en-us</a> |
| %IPV6_DAD_FAILURE: IPv6 Duplicate Address Detected!                                      | Informational | IPv6 duplicate address detected.   | You must configure the hardware <code>l3 ipv6-extended-prefix</code> command globally and reboot the switch to make extended configurations work.   |
| %IPV6_DISABLED_ON_DAD_FAILURE: IPv6 disabled due to Duplicate Address Detection failure. | Informational | IPv6 is disabled due to duplicate address detection failure.   | No action required.   |
| %RA_DNS_OPTION: RDNSS or DNSSL option will no longer be used by IPv6 hosts               | Informational | System log message for RDNSS or DNSSL option configured with zero lifetime to inform the customer that RDNSS or domain name suffix will no longer be used by IPv6 hosts after receiving the RA update. | No action required.   |

# ISCSI system log message reference

This section lists the system log messages that are generated by the iSCSI process.

**Table 24. iSCSI system log messages**

| System log message   | Severity      | Description   | Recommended action   |
|--|---------------|---|--|
| %ISCSI_GLB_ENABLE:<br>ISCSI_OPT: iSCSI Globally enabled. Trigger Auto-config     | Informational | Indicates the configuration of iSCSI Auto-config has been successful. Configurations are going on.  | No action required.  |
| %ISCSI_GLB_DISABLE:<br>ISCSI_OPT: iSCSI Globally disabled.                       | Informational | Indicates disabling of iSCSI Auto config feature.   | No action required.  |
| %ISCSI_STORAGE_PRESENT:<br>ISCSI_OPT: Storage device is connected to switch.     | Informational | Storage device auto-detected based on iSCSI configuration.  | No action required.  |
| %ISCSI_STORAGE_ATTACH:<br>ISCSI_OPT: Storage peer attached to port               | Informational | Dell compliant Storage device such as EQL is detected and attached to the port.   | No action required.  |
| %ISCSI_STP_PORT_FAST:<br>ISCSI_OPT: Auto-config;Set stp port-fast on port        | Informational | Auto-configuration log on setting STP port-fast on Port.  | No action required.  |
| %ISCSI_STORM_CONTROL:<br>ISCSI_OPT: Auto-config;Disable storm control on port    | Informational | On auto configuration log on storm control configuration being removed (if present) on port.  | No action required.  |
| %ISCSI_STORAGE_DETACH:<br>ISCSI_OPT: Storage peer detached from port             | Informational | Dell compliant Storage device such as EQL is detached from port.  | No action required.  |
| %ISCSI_NEW_PORT_FC:<br>ISCSI_OPT: Set flow control for the new port added        | Informational | Log on flow control added for new port added.   | No action required.  |
| %ISCSI_NEW_PORT_MTU:<br>ISCSI_OPT: Set max mtu for the new port added            | Informational | Log on MTU max value set on the port.   | No action required.  |
| %ISCSI_OPT_NEW_TCP_CONN:<br>ISCSI_OPT: New iSCSI Connection Discovered. Src ip   | Informational | New iSCSI session discovered log with IP and port information.  | No action required.  |
| %ISCSI_OPT_ACL_FULL:<br>ISCSI_OPT: Session monitoring ACL Table reservation full | Informational | ACL entries for iSCSI feature gets exhausted. Error Returned during iscsi session monitoring feature. It is not possible to dynamically increase iSCSI space. iSCSI space is static; if the iSCSI space is not enough, You must disable session monitoring. Re-enable the iscsi session monitoring feature again. | No action required.  |
| %ISCSI_OPT_MAX_SESSION_EXCEEDED:<br>ISCSI_OPT: New Connection Ignored            | Informational | Due to ACL restriction number maximum number of session has been exceeded, new connections will get dropped. New session will get established when old sessions gets  | The system has reached its limit. Dell recommends to disable iSCSI session monitoring. |

**Table 24. iSCSI system log messages (continued)**

| System log message        | Severity      | Description   | Recommended action  |
|---------------------------|---------------|---|---------------------|
|                           |               | disabled. Until then they are ignored with this log.                    |                     |
| %ISCSI_APP_TLV: ISCSI_OPT | Informational | Logs on Application TLV to indicate priority on which iSCSI is enabled. | No action required. |

## LACP system log message reference

This section lists the system log messages that are generated by the LACP process.

**Table 25. LACP system log messages**

| System log message   | Severity      | Description   | Recommended action  |
|--|---------------|---|---------------------|
| %LACP_PORT_GROUPED:<br>Interface joined port-channel   | Informational | Port got grouped to port channel.   | No action required. |
| %LACP_PORT_UNGROUPED:<br>Interface exited port-channel   | Informational | Port got ungrouped from port channel.   | No action required. |
| %LACP_INDIVIDUAL_PORT_SPLIT:<br>Individual Port split from port-channel port-channel100 :<br>ethernet1/1/6   | Informational | System log message for information on Individual port split or rejoin actions. This System log message is displayed, when a member-port of port-channel becomes an Individual port. | No action required. |
| %LACP_INDIVIDUAL_PORT_REJOIN:<br>Individual Port rejoined port-channel port-channel100 :<br>ethernet1/1/6  | Informational | This System log message is displayed when an Individual port becomes an active or in-active member of the port-channel interface again.   | No action required. |
| %LACP_INDIVIDUAL: Warning !<br>Enable LACP Individual feature only on port-channel with edge ports. Enabling this on network port-channel could lead to loops :<br>port-channel100           | Informational | This System log message is displayed to warn users about feature configuration.   | No action required. |
| %IFM_LACP_INDIVIDUAL_MODE_CHANGE:<br>Interface is LACP Individual interface now and LACP Mode will be applied when the interface rejoins the Parent Port-channel<br>interface :ethernet1/1/1 | Informational | This System log message is displayed with information about changing the LACP-mode of Individual ports.   | No action required. |



## LADF system log message reference

This section lists the system log messages that are generated by the LADF process.

**Table 26. LADF system log messages**

| System log message   | Severity      | Description   | Recommended action  |
|--|---------------|---|---|
| %LADF_STAG_NOT_FOUND: System service tag not found.              | Critical      | Service Tag not found.  | Contact your technical support representative for further assistance. |
| %LADF_LIC_FILE_NOT_FOUND: License file not present.              | Critical      | If there is no license file present either persistent or evaluation license.  | Install a valid perpetual license.                                    |
| %LADF_LIC_VERIFICATION_FAILED: License file verification failed. | Warning       | License file signature verification failed.   | Install a valid perpetual license.                                    |
| %LADF_LIC_INVALID: Invalid license.                              | Warning       | If it is perpetual license and service-tag, platform type, sw type or sw version doesn't match with installed device this error is thrown.                | Install a valid perpetual license.                                    |
| %LADF_LIC_EVAL_PRD_NOTICE: Evaluation license time limit notice. | Informational | Evaluation license is for 120 days. This log comes if there are only 29 days left for expiry. This is first cut off warning to install perpetual license. | Install a valid perpetual license.                                    |
| %LADF_LIC_EVAL_PRD_EXP: Evaluation license time expiry notice.   | Critical      | Evaluation license is for 120 days is expired.  | Install a valid perpetual license.                                    |
| %LFD_OUT_OF_MEM: LFD: Out of Memory                              | Informational | Not applicable.   | No action required.   |

## LB system log message reference

This section lists the system log messages that are generated by the LB process.

**Table 27. LB system log messages**

| System log Message   | Severity      | Description                                     | Recommended action   |
|--|---------------|---|--|
| %LB_UNEVEN_DISTR: Uneven distribution in link bundle             | Informational | Uneven distribution in link bundle.             | <p>This System log message is seen when traffic distribution on a monitored link is unfairly distributed at given time. If port utilization exceeds the threshold of link bundle:</p> <ul style="list-style-type: none"> <li>• Configure link bundle threshold with higher value using the link-bundle-utilization trigger-threshold command.</li> <li>• Reduce the traffic flow and minimize the port-utilization.</li> </ul> |
| %LB_UNEVEN_DISTR_CLR: Uneven distribution cleared in link bundle | Informational | Uneven distribution got cleared in link bundle. | No action required.  |

## LLDP system log message reference

This section lists the system log messages that are generated by the LLDP process.

**Table 28. LLDP system log messages**

| System log message                               | Severity      | Description                        | Recommended action  |
|--|---------------|------------------------------------|---------------------|
| %LLDP_VIRTUAL_IPV4:<br>LLDP:Virtual IPv4 address | Informational | Displays the virtual ipv4 address. | No action required. |
| %LLDP_VIRTUAL_IPV6:<br>LLDP:Virtual IPv6 address | Informational | Displays the virtual ipv6 address. | No action required. |

## MGMT\_CLISH system log message reference

This section lists the system log messages that are generated by the MGMT\_CLISH process.

**Table 29. MGMT\_CLISH system log messages**

| System log message  | Severity | Description  | Recommended action   |
|---|----------|--|--|
| %MGMT_CLISH_CMD_AAA_AU<br>THOR: Cmd Authorization failed. | Warning  | You are restricted to configure this command with the current user role. When AAA authorization is configured with external servers, these logs will be seen if the command is unauthorized by the remote server for the user. | Remote server can modify the use role to provide access to the user. |

# SFS host tracking system log message reference

This section lists the system log messages generated by the SFS host tracking process.

**Table 30. SFS host tracking system log messages**

| System log message | Severity      | Description   | Recommended action  |
|--------------------|---------------|---|---|
| NVRE9008           | Informational | Information about the host cannot be retrieved because the Host ID entered is unavailable for tracking. | Enter a valid and existing Host tracking ID and retry the operation.      |
| NVRE9009           | Informational | The IP address type or sequence number is missing or invalid.   | Enter a valid IP address type or sequence number and retry the operation. |

## Symmetric hashing system log message reference

This section lists the system log messages that are generated by the Symmetric hashing process.

**Table 31. Symmetric hashing system log messages**

| System log message   | Severity      | Description  | Recommended action  |
|--|---------------|--|---------------------|
| Symmetric hashing and resilient hashing cannot co-exist.   | Informational | You are not allowed to configure symmetric hashing and resilient hashing on Port channel or ECMP. However, you are allowed to configure symmetric hashing on Port channel and resilient hashing on ECMP.                                       | No action required. |
| Enabling symmetric hashing is not allowed when load balancing is enabled for IPv4 or IPv6 VLAN ID protocols fields.  | Informational | Symmetric hashing configuration is not allowed when IPv4 or IPv6 load balancing is enabled for VLAN or protocol fields.  | No action required. |
| Enabling symmetric hashing is not allowed when load balancing is enabled for IPv6 and not for IPv4 SIP and DIP.  | Informational | The Symmetric hashing configuration is allowed only when IPv4 and IPv6 load balancing is enabled for SIP and DIP fields.   | No action required. |
| Enabling symmetric hashing is not allowed when load balancing is enabled for IPv4 and not for IPv6 SIP and DIP.  | Informational | The Symmetric hashing configuration is allowed only when IPv4 and IPv6 load balancing is enabled for SIP and DIP fields.   | No action required. |
| Enabling Symmetric hashing is allowed when load balancing is enabled on SIP and DIP or SIP, DIP, L4SrcPort, or L4DestPort.<br><br>Enabling Symmetric hashing is not allowed when load balancing is enabled only for the source IP address and not for the destination IP address.<br><br>Enabling Symmetric hashing is not allowed when load balancing is enabled only for the destination IP address and not for the source IP address. | Informational | The Symmetric hashing configuration is allowed only when IPv4 and IPv6 load balancing is enabled for the following combinations: <ul style="list-style-type: none"> <li>• SIP and DIP</li> <li>• SIP, DIP, L4SrcPort, and L4DstPort</li> </ul> | No action required. |
| Disabling only IPv4 load balance for L4 ports is not allowed when Symmetric hashing is enabled.<br><br>Disabling only IPv6 load balance for L4 ports is not allowed when Symmetric hashing is enabled.<br><br>Enabling IP load balancing for L4SrcPort or L4DestPort is not allowed when Symmetric hashing is enabled.   | Informational | Disabling of load balancing on the following fields are not allowed when Symmetric hashing is enabled: <ul style="list-style-type: none"> <li>• SIP, DIP, L4SrcPort, and L4DstPort</li> </ul>  | No action required. |

## SyncE ESMC system log message reference

This section lists the system log messages that are generated by the SyncE ESMC process.

When SyncE is enabled on the switch in global and interface levels, if the SyncE input reference (interface) does not get frequency synchronized to any of the available clock sources, an alarm is raised that is displayed in the `show alarms` command. When SyncE input reference (interface) gets frequency synchronized to any of the clock sources, alarms will be cleared.

```
Node.1-Unit.1:PRI [alarm], Dell EMC (OS10) %SyncE_CLOCK_IN_HOLDOVER_STATE: Synchronous Ethernet Clock : Switched to holdover mode. %%ACTION=RAISED %%SEQUENCE=4397

Node.1-Unit.1:PRI [alarm], Dell EMC (OS10) %SyncE_CLOCK_IN_HOLDOVER_STATE: Synchronous Ethernet Clock : Cleared the holdover alarm as frequency lock is acquired. %%ACTION=CLEARED %%SEQUENCE=4397
```

**Table 32. SyncE ESMC system log messages**

| System log message   | Severity      | Description  | Recommended action                              |
|--|---------------|--|---|
| Node.1-Unit.1:PRI [event], Dell EMC (OS10)<br>%SyncE_CLOCK_FREQUENCY_LOCKED: Synchronous Ethernet Clock : Switched to frequency locked mode  | Informational | SyncE input reference (interface) is frequency locked with the SyncE clock source.   | No action required.                             |
| Node.1-Unit.1:PRI [alarm], Dell EMC (OS10)<br>%SyncE_CLOCK_IN_HOLDOVER_STATE: Synchronous Ethernet Clock : Switched to holdover mode. %%ACTION=RAISED %%SEQUENCE=4397                    | Informational | System log message displayed for state of a system to indicate that there is no valid clock source present and SyncE clock in holdover state..   | Verify the clock source or SyncE configuration. |
| % Error: Failed to do forced switch as SyncE is not enabled  | Informational | Error message displayed when we force the switch to SyncE disabled interface.  | No action required.                             |
| % Error: Failed to do <forced/manual> switch as the reference is locked out  | Informational | Error message displayed when we force or manually switch to an interface which is locked-out.  | No action required.                             |
| % Error: Failed to do manual switch as the reference is in forced switch mode  | Informational | Error message displayed when we override a force switch to a manual switch.  | No action required.                             |
| % Error: Failed to do manual switch as the reference is in signal failed state<br>% Error: Failed to do manual switch as the quality level of reference is lower than other reference(s) | Informational | Error message displayed when we manually switch to an interface which is down or in signal-failed state.<br><br>Error message displayed when we manually switch to an interface which has a reference quality level lower than the current active reference (ql-enabled mode). | No action required.                             |
| % Error: Quality level not valid for the SSM network option  | Informational | Error message displayed when the configured quality level on the interface is not a valid value for the configured SSM network or vice-versa.  | No action required.                             |

**Table 32. SyncE ESMC system log messages (continued)**

| <b>System log message</b>  | <b>Severity</b> | <b>Description</b> | <b>Recommended action</b> |
|--|-----------------|--------------------|---------------------------|
| % Error: Mismatch in the SSM network option and quality level configured on references |                 |                    |                           |



## SYSTEM\_MODE\_CHANGE system log message reference

This section lists the system log messages that are generated by the SYSTEM\_MODE\_CHANGE process.

**Table 33. SYSTEM\_MODE\_CHANGE system log messages**

| System log message                          | Severity      | Description  | Recommended action  |
|---|---------------|--|---------------------|
| %SYSTEM_MODE_CHNG:<br>system mode changed : | Informational | Switch operating mode is changed by user. Switch operating mode options are Full-Switch and Smart-Fabric Director. | No action required. |

## SupportAssist - CloudIQ data collection system log message reference

This section lists the system log messages generated by the SupportAssist - CloudIQ data collection process.

**Table 34. Support-Assist - CloudIQ data collection system log messages**

| System log message  | Severity      | Description  | Recommended action   |
|---|---------------|--|--|
| %SA_EVENT_PERFORMANCE_TRANSFER: Support assist performance transfer success | Informational | Indicates that the Support assist performance data transfer is successful. | No action required.  |
| %SA_EVENT_PERFORMANCE_TRANSFER: Support assist performance transfer failed  | Informational | Indicates that the Support assist performance data transfer has failed.    | Verify connectivity to the SupportAssist server. If the connectivity is up, document the message exactly as it appears and contact Dell technical support. |
| %SA_EVENT_FULL_TRANSFER: Support assist full transfer success               | Informational | Indicates that SupportAssist full data transfer is successful.             | No action required.  |
| %SA_EVENT_FULL_TRANSFER: Support assist full transfer failed                | Informational | Indicates that SupportAssist full data transfer has failed.                | Verify connectivity to the SupportAssist server. If the connectivity is up, document the message exactly as it appears and contact Dell technical support. |

## MLD system log message reference

This section lists the system log messages that are generated by the MLD process.

**Table 35. MLD system log messages**

| System log message                           | Severity      | Description  | Recommended action  |
|--|---------------|--|---------------------|
| %MLD_SNOOPING_INTERFACE:<br>MLD Snooping     | Informational | MLD snooping is configured on a default VLAN, hence it is operationally disabled.<br>MLD_SNOOPING_INTERFACE:<br>MLD Snooping disabled on interface :%s | No action required. |
| IGMP or MLD Snooping instance limit receded. | Informational | IGMP or MLD snooping can be enabled on some VLANs.   | No action required. |

## NDM system log message reference

This section lists the system log messages that are generated by the NDM process.

**Table 36. NDM system log messages**

| System log message                                    | Severity      | Description   | Recommended action   |
|---|---------------|---|--|
| %NDM_SYSTEM_RELOAD: User request to reload system     | Informational | You will see this message if you have run the <code>reload</code> command.  | No action required.  |
| %NDM_SPEED_MISMATCH: VLTi member speed doesn't match. | Informational | You will see this message when ports with different speeds are configured as VLT discovery-interfaces. Only ports with matching speeds will be added as VLTi members (port channel 1000. Check "show port-channel summary output). Other ports with different speeds are not added to VLTi. | Identify the member ports of the VLTi configured and remove the member port with mismatched speed. Refer Chapter 22: Virtual Link Trunking->Configure VLT->Configure the VLT in the Dell SmartFabric OS10 User Guide.i |

## PBR match access-list system log message reference

This section lists the system log messages that are generated by the PBR match access-list.

**Table 37. PBR match access-list**

| System log message  | Severity      | Description   | Recommended action  |
|---|---------------|---|---------------------|
| Match access-list not found in the route-map                                | Informational | This system log message is generated when you try to attach an interface for policy based routing to a route map without <code>match access-list</code> criteria.   | No action required. |
| Next-hop IP not set in the route-map  | Informational | This system log message is generated when you try to attach an interface for policy based routing to a routemap without <code>set ip next-hop</code> .  | No action required. |
| Both match access-list and ip next-hop set are not present in the route-map | Informational | This system log message is generated when you try to attach an interface for policy based routing to both <code>match access-list</code> and <code>set ip next-hop</code> which are not configured in a routemap. | No action required. |
| Removing access-list from route-map that is attached with an interface      | Informational | This system log message is generated when you try to unconfigure <code>match access-list</code> from a route-map which has already been attached to an interface.   | No action required. |
| Removing next-hop IP from route-map that is attached with an interface      | Informational | This system log message is generated when you try to unconfigure <code>match access-list</code> from a route-map which has already been attached to an interface.   | No action required. |

## OPEN\_FLOW system log message reference

This section lists the system log messages that are generated by the OPEN\_FLOW process.

**Table 38. OPEN\_FLOW system log messages**

| System log message   | Severity      | Description                            | Recommended action  |
|--|---------------|--|---|
| %OPENFLOW_TABLE_FULL:<br>Openflow table is full : Table ID | Informational | OpenFlow table is full.                | If the table full is not expected, document the message exactly as it appears and contact your technical support representative for assistance. |
| %OPENFLOW_CONTROLLER_STATUS:<br>Openflow Controller        | Informational | OpenFlow controller connection status. | No action required.   |

## OSPFv2 system log message reference

This section lists the system log messages that are generated by the OSPFv2 process.

**Table 39. OSPFv2 system log messages**

| System log message  | Severity      | Description   | Recommended action  |
|---|---------------|---|---|
| %OSPFV2_ADJ_CHANGE: OSPF Process  | Informational | The OSPFv2 session state changes from one state to other state. OSPF Process VRF %s %d, Nbr %s on %s state changed to %s  | No action required.   |
| %OSPFV2_BAD_VERSION: OSPF detected bad version                            | Informational | The received OSPF packet contains wrong version information in OSPF header. OSPF detected bad version VRF %s from %s on interface %s  | Check the version of OSPF process in peer and rectify the same.   |
| %OSPFV2_AREA_MISMATCH: OSPF detected area-id mismatch                     | Informational | The received OSPF packet's source IP address not on same network as receiving interface the area mismatch error is detected. OSPF detected area-id mismatch VRF %s from %s on interface %s        | Check the configured area details in neighbor device or configured IP address of neighbor interface and correct it. |
| %OSPFV2_AUTH_TYPE_MISMATCH: OSPF detected mismatch in authentication type | Informational | The received OSPF packet's authentication method type is not matching with locally configured authentication method. OSPF detected mismatch in authentication type VRF %s from %s on interface %s | Check the configured authentication methods under OSPF interface and correct the configuration.                     |
| %OSPFV2_AUTH_FAILURE: OSPF detected authentication failure                | Informational | The received OSPF packet can not be authenticated. OSPF detected authentication failure VRF %s from %s on interface %s  | Check the configured authentication key in OSPF interfaces and the configured key value should match.               |
| %OSPFV2_NETMASK_MISMATCH: OSPF detected netmask mismatch                  | Informational | The received OSPF hello packet's network mask field does not match with interface's network mask. OSPF detected netmask mismatch VRF %s from %s on interface %s                                   | Check the configured network mask on neighbor interface and configure the correct netmask.                          |
| %OSPFV2_HELLO_INTERVAL: OSPF detected hello interval mismatch             | Informational | The received OSPF hello packet's hello interval value does not match with locally configured hello interval value. OSPF detected hello interval mismatch VRF %s from %s on interface %s           | Check and configure the same hello interval value in OSPF interfaces.   |
| %OSPFV2_DEAD_INTERVAL: OSPF detected dead interval mismatch               | Informational | The received OSPF hello packet's dead interval value does not match with locally configured dead interval value. OSPF detected dead interval mismatch VRF %s from %s on interface %s              | Check and configure the same dead interval value in OSPF interfaces.  |

**Table 39. OSPFv2 system log messages (continued)**

| System log message   | Severity      | Description  | Recommended action  |
|--|---------------|--|---|
| %OSPFV2_OPTION_MISMATCH:<br>OSPF detected option mismatch        | Informational | This indicates there is a mismatch in type of area configuration. OSPF detected option mismatch VRF %s from %s on interface %s   | Check and configure the same area type for OSPFv2 neighbors.  |
| %OSPFV2_MTU_MISMATCH:<br>OSPF detected mtu mismatch              | Informational | The received OSPF hello packet's IP MTU value is not matching with the receiving interface's IP MTU value. The session will stay in EXSTART/ EXCHANGE state. OSPF detected mtu mismatch VRF %s from %s on interface %s                 | Try to configure the same MTU value for ospfv2 interfaces. Otherwise configure ip ospf mtu-ignore command under ospfv2 interfaces to resolve this issue.  |
| %OSPFV2_DUP_RTRID: OSPF detected duplicate router-id             | Informational | The received OSPF packet's router-id is same as of local OSPF router-id. OSPF detected duplicate router-id VRF %s from %s on interface %s  | Check and configure the unique router-id across all ospfv2 routers.   |
| %OSPFV2_NBR_ADMN_DWN:<br>OSPF detected neighbor admin down       | Informational | The OSPFv2 process detected the mentioned neighbor is administratively down. The reason could be interface oper/admin down. Also possible failure in socket creation. OSPF detected neighbor admin down VRF %s from %s on interface %s | Use debug IP ospfv2 command to get the debug prints in journal logs. If there is a socket failure, try to unconfigure and configure again OSPF. If the problem is not resolved reboot the system. If the underlying OSPF interface is admin/ oper down try to activate interface. |
| %OSPFV2_CHNGD_RTRID:<br>OSPF detected change in router-id        | Informational | OSPF process detected change in neighbor's router-id while sending route updates. OSPF detected change in router-id VRF %s from %s on interface %s   | No action required.   |
| %OSPFV2_PKT_LCL_ADDR:<br>OSPF detected packet from local address | Informational | OSPF process detected ospfv2 packet with source IP address as same as OSPFv2 interface's IP address. OSPF detected packet from local address VRF %s from %s on interface %s  | Check and configure STP/RSTP/MSTP wherever needed. Another possible case is using the same IP address for both local and remote ospfv2 interface.   |



## OSPFv3 system log message reference

This section lists the system log messages that are generated by the OSPFv3 process.

**Table 40. OSPFv3 system log messages**

| System log message   | Severity      | Description   | Recommended action   |
|--|---------------|---|--|
| %OSPFV3_ADJ_CHANGE:<br>OSPFv3 Process                            | Informational | The OSPFv3 session state changes from one state to other state. OSPFv3 Process VRF %s %d, Nbr %s on %s state changed to %s  | No action required.  |
| %OSPFV3_BAD_VERSION:<br>OSPF detected bad version                | Informational | The received OSPFv3 packet contains wrong version information in OSPFv3 header OSPF detected bad version VRF %s from %s on interface %s   | Check the version of OSPFv3 process in peer and rectify the same.  |
| %OSPFV3_AREA_MISMATCH:<br>OSPF detected area-is mismatch         | Informational | This indicates there is a mismatch in type of area configuration. OSPF detected area-is mismatch VRF %s from %s on interface %s   | Check and configure the same area type for OSPFv3 neighbors.   |
| %OSPFV3_HELLO_INTERVAL:<br>OSPF detected hello interval mismatch | Informational | The received OSPFv3 hello packet's hello interval value does not match with locally configured hello interval value. OSPF detected hello interval mismatch VRF %s from %s on interface %s                               | Check and configure the same hello interval value in OSPFv3 interfaces.  |
| %OSPFV3_DEAD_INTERVAL:<br>OSPF detected dead interval mismatch   | Informational | The received OSPFv3 hello packet's dead interval value does not match with locally configured dead interval value. OSPF detected dead interval mismatch VRF %s from %s on interface %s                                  | Check and configure the same dead interval value in OSPFv3 interfaces.   |
| %OSPFV3_OPTION_MISMATCH:<br>OSPF detected option mismatch        | Informational | This indicates there is a mismatch in type of area configuration. OSPF detected option mismatch VRF %s from %s on interface %s  | Check and configure the same area type for OSPFv3 neighbors.   |
| %OSPFV3_MTU_MISMATCH:<br>OSPF detected mtu mismatch              | Informational | The received OSPFv3 hello packet's IP MTU value is not matching with the receiving interface's IP MTU value. The session will stay in EXSTART/EXCHANGE state. OSPF detected mtu mismatch VRF %s from %s on interface %s | Try to configure the same MTU value for ospfv3 interfaces. Otherwise configure ipv6 ospf mtu-ignore command under ospfv2 interfaces to resolve this issue. |
| %OSPFV3_DUP_RTRID: OSPF<br>detected duplicate router-id          | Informational | The received OSPFv3 packet's router-id is same as of local OSPF router-id. OSPF detected duplicate router-id VRF %s from %s on interface %s   | Check and configure the unique router-id across all ospfv3 routers.  |
| %OSPFV3_NBR_ADMN_DWN:<br>OSPF detected neighbor admin down       | Informational | The OSPFv3 process detected the mentioned neighbor is administratively down. The reason could be interface  | Use debug ip ospfv3 command to get the debug prints in journal logs. If there  |

**Table 40. OSPFv3 system log messages (continued)**

| System log message   | Severity      | Description  | Recommended action   |
|--|---------------|--|--|
|  |               | oper/admin down. Also possible failure in socket creation. OSPF detected neighbor admin down VRF %s from %s on interface %s  | is a socket failure, try to unconfigure and configure again OSPFv3. If the problem is not resolved reboot the system. If the underlying OSPF interface is admin/oper down try to activate interface. |
| %OSPFV3_CHNGD_RTRID:<br>OSPF detected change in router-id        | Informational | OSPFv3 process detected change in neighbor's router-id while sending route updates. OSPF detected change in router-id VRF %s from %s on interface %s                                       | No action required.  |
| %OSPFV3_PKT_LCL_ADDR:<br>OSPF detected packet from local address | Informational | OSPFv3 process detected received ospfv3 packet contains source IP address as same as OSPFv3 interface's IP address. OSPF detected packet from local address VRF %s from %s on interface %s | Possible loop in router. Check and configure STP/RSTP/MSTP wherever needed. Another possible case is using the same IP address for both local and remote ospfv3 interface.                           |

## Port security system log message reference

This section lists the system log messages that are generated by the Port security process.

**Table 41. Port security system log messages**

| System log message  | Severity      | Description  | Recommended action  |
|---|---------------|--|---------------------|
| Jul 17 10:37:27<br>NPG1 dn_infra_afs[1085]:<br>[INFRA_AFS:MAC-LEARN-LIMIT-<br>VIOLATION], Interface ethernet<br>1/1/1, vlan 200, MAC<br>01:11:11:11:11:11                           | Informational | MAC learn limit violation log. On VLT, violation System log message appears only on the node where violation occurred.         | No action required. |
| Jul 17 10:37:27<br>NPG1 dn_infra_afs[1085]:<br>[INFRA_AFS:MAC-MOVE-<br>VIOLATION], Original Interface:<br>PO 127, Offending<br>Interface: PO128, vlan 100,<br>MAC:00:00:00:00:00:01 | Informational | MAC move violation System log message. On VLT, violation System log message appears only on the node where violation occurred. | No action required. |

## PIM system log message reference

This section lists the system log messages that are generated by the PIM process.

**Table 42. PIM system log messages**


| System log message           | Severity      | Description   | Recommended action   |
|------------------------------|---------------|---|--|
| %PIM_ROUTE: IIF Mismatch For | Informational | There is a mismatch on the incoming interface of a route learnt on the VLT nodes. PIM_ROUTE: IIF Mismatch For SRC: %s GRP: %s, Local IIF %s & Peer IIF %s for VRF: %s Occurred  | Check the PIM interface and VRF level configuration on both the nodes. |
| %PIM_INTERFACE: PIM          | Informational | PIM is configured on a default VLAN, hence it is operationally disabled. PIM_INTERFACE: PIM disabled on interface :%s   | No action required.  |
| %PIM_PURGE_DELAY_START_TIMER | Informational | Synced multicast routes received from the peer are retained for a duration of the configured timer during a VLT peer node failure. The following message indicates that timer started for retaining the routes. PIM detected multicast peer-routing timer start                     | No action required.  |
| %PIM_PURGE_DELAY_STOP_TIMER  | Informational | Synced multicast routes received from the peer are retained for duration of the configured timer during a VLT peer node failure. The following message indicates that timer stopped and all stale multicast entries are removed. PIM detected multicast peer-routing timer stop     | No action required.  |
| %PIM_PURGE_DELAY_START_TIMER | Informational | Synced multicast routes received from peer are retained for duration of the configured timer during a VLT peer node failure. The following message indicates that the timer has started for retaining the routes: PIM detected multicast peer-routing timer start                   | No action required.  |
| %PIM_PURGE_DELAY_STOP_TIMER  | Informational | Synced multicast routes received from peer are retained for duration of the configured timer during a VLT peer node failure. The following message indicates that the timer has stopped and all stale multicast entries are removed: PIM detected multicast peer-routing timer stop | No action required.  |

# PKI certificate system log message reference

This section lists the system log messages that are generated by the PKI certificate process.

An audit log message is generated with the result of the validation, which is either a success or failure. If a failure occurs, then the reason for that failure is present in the audit log message.

System can only evaluate the certificate or key files as presented.

 **NOTE:** You can use the information embedded in the System log message to mitigate the problem or issue that the System log message indicates.

**Table 43. PKI certificate system log messages**

| System log message   | Severity      | Description                  | Recommended action  |
|--|---------------|------------------------------|---------------------|
| CA certificate with CN = <commonName from certificate> successfully deleted  | Informational | CA certificate deletion.     | No action required. |
| CA certificate with CN = <commonName from certificate> successfully installed<br><br>Trusted server certificate with CN = <commonName from certificate> successfully installed<br><br>CA certificate failed to install. <error output>" where error output could be: <ul style="list-style-type: none"> <li>• %% Error: NULL file pointer</li> <li>• %% Error: X509 allocation failure</li> <li>• %% Error: X509 certificate file can only contain one certificate</li> <li>• %% Error: invalid PEM certificate</li> <li>• %% Error: no installable certificate</li> <li>• %% Error: Unable to open certificate file</li> <li>• %% Error: Certificate already exists in internal certificate directory</li> <li>• %% Error: Unable to validate trusted-host certificate file</li> <li>• %% Error: Unable to validate CA certificate file</li> <li>• %% Error: Unable to create certificate directory</li> <li>• %% Error: Unable to copy certificate file to internal certificate directory</li> <li>• %% Error: Unable to create certificate store directory</li> <li>• %% Error: Unable to successfully add certificate</li> </ul> | Informational | CA certificate installation. | No action required. |

**Table 43. PKI certificate system log messages (continued)**

| System log message  | Severity      | Description               | Recommended action  |
|---|---------------|---------------------------|---------------------|
| <p>CDP with name = &lt;filename&gt; successfully installed</p> <p>CDP with name = &lt;filename&gt; successfully deleted</p>   | Informational | CDP addition or deletion. | No action required. |
| <p>Certificate failed to validate - failed to open certificate file</p> <p>Certificate failed to validate - invalid certificate file</p> <p>Certificate with CN = &lt;commonName from certificate&gt; failed to validate - certificate is not yet valid</p> <p>Certificate with CN = &lt;commonName from certificate&gt; failed to validate - certificate is expired</p> <p>Self-signed certificate with CN = &lt;commonName from certificate&gt; verified successfully</p> <p>Certificate with CN = &lt;commonName from certificate&gt; failed verification - &lt;error output&gt;" where error output could be:</p> <ul style="list-style-type: none"> <li>• unable to create verification context</li> <li>• unable to read file</li> <li>• no usable trust store</li> <li>• chain invalid at cert# &lt;# of failed cert in chain&gt;: &lt;error output&gt;" where error output comes from OpenSSL errors "Certificate verified &lt;details&gt;" where details could be: <ul style="list-style-type: none"> <li>○ but certificate is revoked</li> <li>○ and certificate is not revoked</li> <li>○ but certificate is unknown to OCSP responder</li> <li>○ CRL not present. Accepting certificate</li> <li>○ But certificate is revoked</li> <li>○ Certificate is not revoked</li> <li>○ Certificate with CN = &lt;commonName from certificate&gt; verified successfully</li> <li>○ Certificate failed to validate - unable to access certificate &lt;filename&gt;</li> </ul> </li> </ul> | Informational | Certificate validation.   | No action required. |
| <p>Unable to successfully remove all CRLs</p> <p>All CRLs successfully deleted</p>  | Informational | CRL deletion.             | No action required. |

**Table 43. PKI certificate system log messages (continued)**

| System log message  | Severity      | Description                    | Recommended action  |
|---|---------------|--------------------------------|---------------------|
| CRL not found<br>Unable to delete CRL file<br><filename><br>Unable to successfully remove<br>CRL<br>CRL deleted for issuer:<issuer<br>commonName from issuer<br>certificate> CRL Number: <# of<br>CRL>  |               |                                |                     |
| Unable to open CRL file<br>CRL with the same name already<br>exists<br>Unable to copy file to CRL<br>directory<br>CRL installed for issuer:<issuer<br>commonName from issuer<br>certificate>. CRL Number: <# of<br>CRL><br>Unable to convert DER CRL to<br>PEM<br>CRL installed for issuer:<issuer<br>commonName from issuer<br>certificate>. CRL Number: <# of<br>CRL><br>invalid CRL file<br>Unable to successfully add CRL   | Informational | CRL Installation.              | No action required. |
| Host certificate with CN =<br><commonName from certificate><br>successfully deleted<br>Key for certificate with CN =<br><commonName from certificate><br>successfully deleted. Key hash<br><hash>   | Informational | Host certificate deletion.     | No action required. |
| Host certificate/key failed to<br>install - failed to open key file<br>Host certificate/key failed to<br>install - failed to open certificate<br>file<br>Host certificate/key failed to<br>install - invalid key file<br>Host certificate/key failed to<br>install - invalid certificate file<br>Host certificate/key failed to<br>install - CA flag is true in host<br>certificate CN = <commonName<br>from certificate><br>Host certificate/key failed to<br>install - FIPS mode certificate<br>CN = <commonName from<br>certificate> must be RSA | Informational | Host certificate installation. | No action required. |

**Table 43. PKI certificate system log messages (continued)**

| System log message  | Severity | Description | Recommended action |
|---|----------|-------------|--------------------|
| Host certificate/key failed to install - certificate CN = <commonName from certificate> is not yet valid      |          |             |                    |
| Host certificate/key failed to install - certificate CN = <commonName from certificate> is expired            |          |             |                    |
| Host certificate/key failed to install - invalid certificate/key pair CN = <commonName from certificate>      |          |             |                    |
| Host certificate CN = <commonName from certificate> and keypair verified successfully                         |          |             |                    |
| Host certificate/key failed to install. Unable to open certificate file <filename>                            |          |             |                    |
| Host certificate/key failed to install. Private Keyfile does not exist  |          |             |                    |
| Host certificate/key failed to install. Keyfile does not exist  |          |             |                    |
| Host certificate/key failed to install. Keyfile is encrypted but no password provided to decrypt it           |          |             |                    |
| Host certificate/key failed to install. Keyfile is not encrypted but password has been provided to decrypt it |          |             |                    |
| Host certificate/key failed to install. Failed to decrypt private keyfile                                     |          |             |                    |
| Host certificate/key failed to install. Unable to create storage location for certificate                     |          |             |                    |
| Host certificate/key failed to install. Unable to create storage location for key                             |          |             |                    |
| Host certificate/key failed to install. Unable to create storage location for FIPS certificate                |          |             |                    |
| Key for certificate with CN = <commonName from certificate> successfully installed                            |          |             |                    |
| Host certificate with CN = <commonName from certificate> successfully added. Key hash <hash>                  |          |             |                    |
| Host certificate/key failed to install. Unable to access certificate <filename>                               |          |             |                    |



**Table 43. PKI certificate system log messages (continued)**

| System log message  | Severity | Description | Recommended action |
|---|----------|-------------|--------------------|
| Host certificate/key failed to install. Unable to access key file<br>Host certificate failed certificate chain validation. Not installing certificate/key |          |             |                    |

## PTP system log message reference

This section lists the system log messages that are generated by the PTP process.

**Table 44. PTP system log messages**

| System log message  | Severity      | Description   | Recommended action   |
|---|---------------|---|--|
| %PTP_CLOCK_PHASE_LOCKED : Clock servo is phase locked.                  | Informational | Lock status of the clock is phase locked with master. This means that the offset with the master is within the default range of +/- 1 micro seconds. Lock status of the clock is phase locked with master. This means that the offset with the master is within the default range of +/- 1 micro seconds.   | No action required.  |
| %PTP_CLOCK_PHASE_LOCK_EXPIRED: Clock servo is out of phase lock.        | Informational | Lock status of the clock is out of lock with master clock. This indicates the loss of master clock or config change. In the case of losing master clock, clock runs either in holdover mode or switch to other master. Lock status of the clock is out of lock with master clock. This indicates the loss of master clock or config change. In the case of losing master clock, clock runs either in holdover mode or switch to other master. | Check the network connection if this loss of master is not intended. |
| %PTP_PORT_ROLE_CHANGED: Port role changed.                              | Informational | Indicates the role of a specific PTP port is changed to SLAVE.  | No action required.  |
| %PTP_PORTS_LIMIT_REACHED : Ports limit reached.                         | Informational | Number of configured ports reached the system supported limit..   | No action required.  |
| %PTP_SLAVES_LIMIT_REACHED: Slaves limit reached.                        | Informational | Number of configured unicast slaves reached the system supported limit. Number of configured unicast slaves reached the system supported limit.   | No action required.  |
| %PTP_MASTERS_LIMIT_REACHED: Masters limit reached.                      | Informational | Number of configured unicast masters reached the system supported limit. Number of configured unicast masters reached the system supported limit.   | No action required.  |
| %PTP_SYSTEM_TIME_NOT_SET: System time is not set.                       | Informational | Indicates that the system time is not set currently as the clock is not phase locked with master. System time will be set when the clock is phase locked. Indicates that the system time is not set currently as the clock is not phase locked with master. System time will be set when the clock is phase locked.   | No action required.  |
| %PTP_SYSTEM_TIME_UPDATE_STARTED: System time update service is started. | Informational | Indicates that the system time update service is started and would update the system time at regular intervals. Indicates that the system time update   | No action required.  |

**Table 44. PTP system log messages (continued)**

| System log message  | Severity      | Description   | Recommended action  |
|---|---------------|---|---------------------|
|   |               | service is started and would update the system time at regular intervals.   |                     |
| %PTP_SYSTEM_TIME_UPDATE_STOPPED: System time update service is stopped. | Informational | Indicates that the system time update service is stopped. This happens either upon config change or lock status change. Indicates that the system time update service is stopped. This happens either upon config change or lock status change. | No action required. |

## QoS system log message reference

This section lists the system log messages that are generated by the QoS process.

**Table 45. QoS system log messages**

| System log message   | Severity | Description  | Recommended action  |
|--|----------|--|---|
| %QOS_PFC_SERVICE_POLICY:<br>Pfc service policy:            | Warning  | When a network qos policy, which has Priority Flow Control enabled is attached to an interface having Link Level Flow Control (LLFC) receive or transmit enabled, the system log is generated. The system log is not being used.   | Disable both Link Level Flow Control (LLFC) receive and transmit configurations before attaching the Priority Flow Control enabled network qos policy on the interface. |
| %QOS_BUFFER_INIT_FAIL:<br>Buffer initialization has failed | Critical | As part of the switch initialization sequence each interface is allocated a dedicated amount of buffer based on the interface speed. If there is a failure in the buffer initialization this system log is generated. The failure could happen during port breakout, break in also.  | Document the message exactly as it appears and contact your technical support representative for assistance.  |
| %QOS_COPP_LIMIT_MAX:<br>Control plane policy:              | Warning  | There are multiple queues carrying the control traffic towards the CPU. Each queue is assigned a rate-limit based on the priority of the control traffic which flows through it. There is a cumulative rate-limit of all the queues beyond which the system behavior may become undefined. The system log is generated when the cumulative rate limit of the control packets towards the CPU exceeds the per platform cumulative rate. | Ensure that cumulative rate limit for the CPU queues doesn't exceed the recommended value.  |

## RAGUARD\_EVENT system log message reference

This section lists the system log messages that are generated by the RAGUARD\_EVENT process.

**Table 46. RAGUARD\_EVENT system log messages**

| System log message                                   | Severity      | Description  | Recommended action   |
|--|---------------|--|--|
| %RAGUARD_DENIED_RA_PACKET: RAGUARD: Denied RA Packet | Informational | Received Router Advertisement packet is dropped because of policy mismatch. RAGuard policy can be configured to prevent attacks based on RA messages. The received RA packet will be validated against the configured RAGuard policy and it will either be allowed or dropped. | If an RA packet is dropped, you need to revisit the RAGuard policy to find out whether the RA packet is genuine or the RA packet is being used to attack the system. |

## RAGUARD system log message reference

This section lists the system log messages that are generated by the RAGUARD process.

**Table 47. RAGUARD system log messages**

| System log message | Severity      | Description   | Recommended action   |
|--------------------|---------------|---|--|
| % RAGUARD          | Informational | IPv6 RA Guard is enabled on the interface, so BGP unnumbered configuration on the same will not work. | It indicates that RA Guard is enabled on the interface where BGP unnumbered session is up. Since RA Guard feature has high priority, BGP unnumbered session is down. |

## Routemap with match ACL system log message reference

This section lists the system log message for route-map with match ACL when added to routing protocol per VRF from OS10 release 10.5.2.3.

**Table 48. Routemap with match ACL**

| System log message   | Severity      | Description   | Recommended action  |
|--|---------------|---|---------------------|
| Route-map <rmap_name>: Match address based on ACL is not applicable for Routing modules in VRF <vrf_name>. | Informational | This system log message is generated when a route-map with match ACL is added to VRF or BGP for the first time. This message is also generated and when configuring match ACL in a route-map which is part of VRF or BGP. | No action required. |

# Scale VLAN profile system log message reference

This section lists the system log message for Scale VLAN Profile and L3 configuration when L3 mode is not configured from OS10 release 10.5.2.3.

**Table 49. Scale VLAN profile**

| System log message  | Severity | Description   | Recommended action   |
|---|----------|---|--|
| %SCALED_VLAN_PROFILE:<br>Scaled VLAN Profile<br>Configuration: Mode L3<br>configuration needs to be enabled<br>for configuring IPv4 Address in<br>Scaled VLAN profile         | Warning  | This system log message is generated when an IPv4 address is configured on the VLAN interface with scale VLAN profile, which is globally enabled and L3 mode is not configured.         | Configure and enable mode L3 to configure IPv4 address in a scaled VLAN profile. For more information on configuring scaled VLAN profile, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us</a>        |
| %SCALED_VLAN_PROFILE:<br>Scaled VLAN Profile<br>Configuration: Mode L3<br>configuration needs to be enabled<br>for configuring IPv6 Address in<br>Scaled VLAN profile         | Warning  | This system log message is generated when IPv6 address is configured on a VLAN interface with scale VLAN profile, which is globally enabled and L3 mode is not configured.              | Configure and enable mode L3 to configure IPv6 address in a scaled VLAN profile. For more information on configuring scaled VLAN profile, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us</a>        |
| %SCALED_VLAN_PROFILE:<br>Scaled VLAN Profile<br>Configuration: Mode L3<br>configuration needs to be enabled<br>for configuring Anycast IPv4<br>Address in Scaled VLAN profile | Warning  | This system log message is generated when an Anycast IPv4 address is configured on the VLAN interface with Scale VLAN profile, which is globally enabled and L3 mode is not configured. | Configure and enable mode L3 to configure anycast Pv4 address in a scaled VLAN profile. For more information on configuring scaled VLAN profile, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us</a> |
| %SCALED_VLAN_PROFILE:<br>Scaled VLAN Profile<br>Configuration: Mode L3  | Warning  | This system log message is generated when an Anycast IPv6 address is configured on a VLAN interface with  | Configure and enable mode L3 to configure IPv6 address in a scaled   |



**Table 49. Scale VLAN profile (continued)**

| System log message  | Severity | Description   | Recommended action   |
|---|----------|---|--|
| configuration needs to be enabled for configuring Anycast IPv6 Address in Scaled VLAN profile   |          | Scale VLAN profile, which is globally enabled and L3 mode is not configured.  | VLAN profile. For more information on configuring scaled VLAN profile, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us</a>   |
| %SCALED_VLAN_PROFILE: Scaled VLAN Profile Configuration: Mode L3 configuration needs to be enabled for VRF association in Scaled VLAN profile             | Warning  | This system log message is generated when a VRF is associated on the VLAN interface with Scale VLAN profile, which globally enabled and L3 mode is not configured.                                    | Configure and enable mode L3 to associate a VRF to a scaled VLAN profile. For more information on configuring scaled VLAN profile, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us</a>           |
| %SCALED_VLAN_PROFILE: Scaled VLAN Profile Configuration: Mode L3 configuration needs to be enabled for configuring VRRP IPv4 Group in Scaled VLAN profile | Warning  | This system log message is generated when Virtual IPv4 address of VRRP V4 Group is configured on the VLAN interface with Scale VLAN profile, which is globally enabled and L3 mode is not configured. | Configure and enable mode L3 to configure VRRP IPv4 group in a scaled VLAN profile. For more information on configuring scaled VLAN profile, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us</a> |
| %SCALED_VLAN_PROFILE: Scaled VLAN Profile Configuration: Mode L3 configuration needs to be enabled for configuring VRRP IPv6 Group in Scaled VLAN profile | Warning  | This system log message is generated when Virtual IPv6 address of a VRRP V6 Group is configured on a VLAN interface with Scale VLAN profile, which globally enabled and L3 mode is not configured.    | Configure and enable mode L3 to configure VRRP IPv6 group in a scaled VLAN profile. For more information on configuring scaled VLAN profile, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us</a> |
| %SCALED_VLAN_PROFILE: Scaled VLAN Profile Configuration: Mode L3 configuration needs to be enabled  | Warning  | This system log message is generated when NTP is disabled on a VLAN interface with Scale VLAN profile, which is globally enabled and L3 mode is not configured.                                       | Configure and enable mode L3 to disable NTP in a scaled VLAN profile. For more information on configuring scaled VLAN profile,   |

**Table 49. Scale VLAN profile (continued)**

| System log message                       | Severity | Description | Recommended action  |
|--|----------|-------------|---|
| for disabling NTP in Scaled VLAN profile |          |             | see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/mode-l3?guid=guid-1af511a6-ea2f-491b-a619-fd8ed238104f&amp;lang=en-us</a> |

## Static and dynamic route system log message reference

This section lists the system log message for static and dynamic route with prefix greater than 64 and less than 128 when the IPv6 extended prefix is not configured from OS10 release 10.5.2.1.

**Table 50. Static and dynamic route**

| System log message   | Severity      | Description   | Recommended action  |
|--|---------------|---|---|
| IPv6 Extended Prefix support not configured - Unable to program routes with prefix length greater than 64 and less than 128. | Informational | This system log message is generated when you try to attach a program to IPv6 route with prefix length greater than 64 and less than 128 when IPv6 extended prefix is not configured. | You must configure hardware I3 IPv6 extended prefix or else addresses greater than / 64 will not be programmed. For more information on configuring IPv6-extended prefix, see <a href="https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/hardware-l3-ipv6-extended-prefix?guid=guid-889ed6e9-9728-49e4-9a7c-d35f80663188&amp;lang=en-us">https://www.dell.com/support/manuals/en-us/dell-emc-smartfabric-os10/smartfabric-os-user-guide-10-5-2/hardware-l3-ipv6-extended-prefix?guid=guid-889ed6e9-9728-49e4-9a7c-d35f80663188&amp;lang=en-us</a> |

## SA system log message reference

This section lists the system log messages that are generated by the SA process.

**Table 51. SA system log messages**

| System log message  | Severity      | Description  | Recommended action  |
|---|---------------|--|---|
| %SUPPORTASSIST_SERVICE_UP: Support Assist Service up                            | Informational | Support Assist Service is enabled by the user.             | No action required.   |
| %SA_ACTI_FULL_XFER_SUCCESS: Support Assist Full Transfer completed successfully | Informational | Uploaded the complete bundle to support assist server.     | No action required.   |
| %SA_ACTI_FULL_XFER_FAILURE: Support Assist Full Transfer failed                 | Informational | Failed to upload complete bundle to support assist server. | Verify the connectivity to support assist server. If the connectivity is up, document the message exactly as it appears and contact your technical support representative for assistance. |
| %SA_ACTI_LOG_XFER_SUCCESS: Support Assist Log Transfer completed successfully   | Informational | Uploaded logs files to support assist server.              | No action required.   |
| %SA_ACTI_LOG_XFER_FAILURE: Support Assist Log Transfer failed                   | Informational | Failed to upload logs files to support assist server.      | Verify the connectivity to support assist server. If the connectivity is up, document the message exactly as it appears and contact your technical support representative for assistance. |

## Scheduled reload system log message reference

This section lists the system log messages that are generated by the Scheduled reload process.

**Table 52. Scheduled reload system log messages**

| System log message  | Severity      | Description  | Recommended action  |
|---|---------------|--|---------------------|
| %NDM_SYSTEM_SCHEDULED_RELOAD: Scheduled reload is aborted as image install is in progress   | Informational | If the image install is in progress , this system log message is displayed when the switch cannot be reloaded at the scheduled time.   | No action required. |
| %NDM_SYSTEM_SCHEDULED_RELOAD: Startup configuration changed after secure boot protection.Please protect startup configuration before scheduled reload | Informational | If the secure boot startup configuration protect validation fails, this System log message is displayed to notify you to protect the startup configuration file before the scheduled reload is triggered.  | No action required. |
| %NDM_SYSTEM_SCHEDULED_RELOAD: Scheduled reload is aborted as startup configuration is changed after secure boot protection                            | Informational | If the secure boot startup configuration protect validation fails, this System log message is displayed when the switch cannot be reloaded at the scheduled time.  | No action required. |
| %NDM_SYSTEM_SCHEDULED_RELOAD: Scheduled reload is aborted as system time change skipped reload time   | Informational | This System log message is displayed when the switch local time is changed to a later time, skipping the configured reload time, notifying the user that the scheduled reload is cancelled.  | No action required. |
| %NDM_SYSTEM_SCHEDULED_RELOAD: Reload scheduled at Wed Sep 1 16:32:00 2021 UTC.User request to reload the system                                       | Informational | This System log message is displayed when the switch goes for reboot at the scheduled time.  | No action required. |
| %NDM_SYSTEM_SCHEDULED_RELOAD: Reload scheduled at Wed Sep 1 15:33:25 2021 UTC. Please save any unsaved changes to startup-configuration               | Informational | When Scheduled reload is configured, this System log message is displayed periodically notifying the user per day. Before the last 24 hours from the Scheduled reload time, System log messages are generated per hour. Before the last hour from the Scheduled reload time, System log messages are displayed at 30 minutes, 5 minutes, 2 minutes, and 30 seconds interval. | No action required. |

## STATIC\_MGMTsystem log message reference

This section lists the system log messages that are generated by the STATIC\_MGMT process.

**Table 53. STATIC\_MGMT system log messages**

| System log message  | Severity      | Description  | Recommended action  |
|---|---------------|--|---------------------|
| %STATIC_MGMT_ROUTE_OVE<br>RWRITE: Overriding static route<br>with route obtained via DHCP/<br>Autoconf. | Informational | Static Route configured is overridden by<br>route via DHCP/AutoConf. | No action required. |

## STP system log message reference

This section lists the system log messages that are generated by the STP process.

**Table 54. STP system log messages**

| System log message   | Severity      | Description  | Recommended action   |
|--|---------------|--|--|
| %STP_BPDU_GUARD_ERR:<br>STP: BPDU received on BPDU guard enabled port.   | Informational | The spanning-tree bpduguard enable command is configured on an interface(s) and OS10 is reporting that the interface received a BPDU. The interface is brought down and placed in ERR_DISABLE mode. BPDU received on BPDU guard enabled port.%s  | Remove the device which is transmitting STP BPDU to the BPDU guard enabled port and place an edge device.                                    |
| %STP_BPDU_GUARD_CLR:<br>STP: BPDU Guard violation cleared.               | Informational | BPDU guard enabled port stopped receiving STP BPDU from peer device. BPDU Guard violation cleared.%s   | No action required.  |
| %STP_MAX_INST_REACHED:<br>STP: Spanning tree maximum instance            | Critical      | Rapid-PVST per VLAN STG instance reached the hardware limit. After this system log, Rapid-PVST cannot allocate new STG instance for the new VLANs being created. Spanning tree maximum instance %d reached.  | Change the STP mode to RSTP or MSTP. You can change the mode to RSTP or MSTP using the spanning-tree mode {rstp   mst   rapid-pvst} command. |
| %STP_FREE_INST_AVAILABLE:<br>STP: Spanning tree free instance available. | Informational | Free HW STG instances are available and RPVST can allocate/use the free STG instance for further VLANs configured. Spanning tree free instance available.  | No action required.  |
| %STP_ROOT_CHANGE:<br>STP:Root Brg Chg                                    | Informational | STP root bridge is changed. If the active STP flavor is RPVST: RPVST root changed for vlan %d. My ID:%sOldRt:%s NewRt:%s If the active STP flavor is MSTP: MSTP root changed for instance %d. My ID:%sOldRt:%s NewRt:%s If the active STP flavor is RSTP: RSTP root changed. My ID:%sOldRt:%s NewRt:%s | No action required.  |

## UFD system log message reference

This section lists the system log messages that are generated by the UFD process.

**Table 55. UFD system log messages**

| System log message  | Severity      | Description   | Recommended action  |
|---|---------------|---|---------------------|
| %UFD_ERROR_SET: Interface set to UFD Error :                                | Informational | This log is displayed when the downstream interface is set to disabled due to upstream interfaces going down.   | No action required. |
| %UFD_ERROR_CLR: Interface cleared from UFD Error :                          | Informational | This log is displayed when the upstream interfaces come up or when you execute the <code>clear ufd-disable uplink-state-group &lt;1&gt;</code> command, which will clear the downstream interface from disabled state.. | No action required. |
| %UFD_GRP_ERROR_SET: Uplink State Group moved to Error state - Group id:     | Informational | This log is displayed when the port channel member interface is added to the Uplink state group.  | No action required. |
| %UFD_GRP_ERROR_CLR: Uplink State Group moved out of Error state - Group id: | Informational | This log is displayed when the port channel member interface is removed from the Uplink state group.  | No action required. |



# USER\_ROLE\_CHANGED system log message reference

This section lists the system log messages that are generated by the USER\_ROLE\_CHANGED process.

**Table 56. USER\_ROLE\_CHANGED system log messages**

| System log message                    | Severity      | Description   | Recommended action  |
|---------------------------------------|---------------|---|---------------------|
| %USER_ROLE_CHANGE: User role changed. | Informational | Information to user about user role change(helpful when user role is modified in remote authentication servers). Informational. | No action required. |

## Delay restore port system log message reference

This section lists the system log messages that are generated by the Delay restore port process.

**Table 57. Delay restore port system log messages**

| System log message  | Severity      | Description  | Recommended action  |
|---|---------------|--|---------------------|
| %DELAY_RESTORE_PORT_START: Delay restore port timer start   | Informational | Indicates that delay restore timer has started for ports after reload. Delay restore port is used for non-VLT deployments. The configured ports are kept down on system boot up (after a reload) and are brought up only after the configured delay restore port timer expiry. This timer is different from VLT's delay restore timer. | No action required. |
| %DELAY_RESTORE_PORT_COMPLETE: Delay restore port timer stop | Informational | Indicates delay restore timer completion for ports after reload. Once the timer completes, the down ports which are enabled with delay-restore are brought up.   | No action required. |

## VLT system log message reference

This section lists the system log messages that are generated by the VLT process.

**Table 58. VLT system log messages**

| System log message                         | Severity      | Description   | Recommended action   |
|--|---------------|---|--|
| %VLT_ELECTION_ROLE: VLT                    | Informational | Indicates that VLT node(s) in a VLT domain elected a role. Local and remote VLT nodes can be distinguished using a unit number present in the system log. Whenever a VLT node elects a role afresh, system log will appear in the following format unit %d is elected as %s In case a VLT node role transitions from current role to new role, system log will appear like unit %d role transitioned from %s to %s. | No action required.  |
| %VLT_VLTi_LINK_UP: VLT interconnect link   | Informational | Indicates that virtual link trunk interconnect (VLTi) link is operationally up. VLT interconnect link between unit %d and unit %d is up   | No action required.  |
| %VLT_VLTi_LINK_DOWN: VLT interconnect link | Critical      | Indicates that virtual link trunk interconnect (VLTi) link is operationally down. VLT interconnect link between unit %d and unit %d is down.  | If the VLTi is down without any user intervention (i.e shutting down discovery interfaces manually), collect the show tech-support (apply CodeText to this command) command output, save the report, and contact technical support for assistance. |
| %VLT_PEER_UP: VLT                          | Informational | Indicates that VLT peer node is UP. VLT unit %d is up.  | No Action required.  |
| %VLT_PEER_DOWN: VLT                        | Informational | Indicates that VLT peer node is down or disconnected. VLT unit %d is down.  | If the peer node is down or removed from the VLT domain without any user intervention, collect the show tech-support (apply CodeText to the command name) command output, save the report, and contact Technical Support for assistance.           |
| %VLT_VLT_MAC_MISMATCH: VLT mac mismatch    | Informational | Indicates that different VLT MAC addresses are configured in VLT peers. In case a different VLT MAC address is configured in the VLT peer, following system log will  | Configure the same VLT MAC in both the VLT peers.  |

**Table 58. VLT system log messages (continued)**

| System log message   | Severity      | Description  | Recommended action   |
|--|---------------|--|--|
|  |               | appear on the console, detected for unit %u. Here unit represents the VLT peer unit id. After the detection of VLT MAC mismatch, If user configures the same MAC in the other VLT peer as well, following system log will appear cleared for unit %u   |  |
| %VLT_PORT_CHANNEL_UP: vlt-port-channel                       | Informational | VLT port-channel is operationally UP in one of the VLT peers. vlt-port-channel %d is up.   | No action required.  |
| %VLT_PORT_CHANNEL_DOWN : vlt-port-channel                    | Informational | VLT port channel is down in both of the VLT peers. vlt-port-channel %d is down.  | If the VLT port-channel is down without any user intervention, collect the show tech-support (apply CodeText to command name) command output, save the report, and contact Technical Support for assistance. . |
| %VLT_ACL_ERROR: VLT ACL CAM table full                       | Warning       | Indicates that VLT application can not program data forwarding rules in the hardware. VLT ACL CAM table full.  | No action required.  |
| %VLT_HB_UP: VLT peer heartbeat link is up                    | Informational | Indicates that VLT heart beat or backup link is up. VLT peer heartbeat link is up .  | No action required .   |
| %VLT_HB_DOWN: VLT peer heartbeat link is down                | Critical      | Indicates that VLT heart beat or backup link is down. VLT peer heartbeat link is down.   | If a backup link is down without user intervention, collect the show tech-support command output , SOS report and contact technical support representative.  |
| %VLT_DELAY_RESTORE_START: VLT delay restore timer start      | Informational | Indicates that Delay restore timer is started. Before the timer is started, all the VLT port-channels in the secondary node are brought down. This timer is started only in the VLT secondary node to delay the restoration of services on VLT secondary VLT port-channels. Newly configured VLT port-channels will also be brought down when this timer is active. VLT delay restore timer start. | No action required.  |
| %VLT_DELAY_RESTORE_COMPLETE: VLT delay restore timer stop    | Informational | Delay restore timer is stopped or expired. After the expiry of this timer, VLT port-channels will be brought up. VLT delay restore timer stop.   | No action required.  |
| %VLT_SOFTWARE_VERSION_MISMATCH:VLT software version mismatch | Informational | Indicates that there is a mismatch in VLT internal software versions between the VLT peers.  | Load the VLT peers with installer that consists of the same VLT version.   |
| %VLT_PORT_ERROR_DISABLE D: VLT port                          | Informational | Indicates that the VLT port channel is put in error-disabled state or the VLT port channel recovered from an   | If the VLT port-channel is put in error-disabled state,  |

**Table 58. VLT system log messages (continued)**

| System log message | Severity | Description  | Recommended action                         |
|--------------------|----------|--|--|
|                    |          | error disabled state. If the VLT port channel it is put in error disabled state the following message appears: VLT port 10 is put in error-disabled state pending egress mask installation in remote peer. If the VLT port channel recovers from the error-disabled state, then the following message appears: VLT port 10 recovered from error-disabled state. The VLT port channel is down when it is put in error-disabled state; the VLT port channel comes up when it recovers. | then collect the show tech support output. |

## VRF system log message reference

This section lists the system log messages that are generated by the VRF process.

**Table 59. VRF system log messages**

| System log message                       | Severity      | Description   | Recommended action  |
|--|---------------|---------------|---------------------|
| %VRF_CREATE: VRF Creation is successful. | Informational | VRF Creation. | No action required. |
| %VRF_DELETE: VRF Deletion is successful. | Informational | VRF Deletion. | No action required. |

## VXLAN system log message reference

This section lists the system log messages that are generated by the VXLAN process.

**Table 60. VXLAN system log messages**

| System log message   | Severity      | Description   | Recommended action  |
|--|---------------|---|---|
| %VXLAN_OVERLAY_ECMP_PROFILE_MODIFIED: VxLAN Overlay ECMP:  | Informational | Hardware overlay-ecmp-profile mode configuration is changed. Configuration is modified, Save and Reload the device for the profile to be effective.   | To take effect, system configurations should be saved and reloaded. |
| %VXLAN_OVERLAY_ECMP_PROFILE_APPLIED: VxLAN Overlay ECMP:   | Informational | Hardware overlay-ecmp-profile mode configuration is getting applied in the HW during system booting.  | No action required.   |
| %VXLAN_OVERLAY_ROUTING_PROFILE_MODIFIED: VxLAN Overlay Routing:  | Informational | Hardware overlay-routing-profile configuration has changed. Configuration is modified, Save and Reload the device for the profile to be effective.  | To take effect, system configurations should be saved and reloaded. |
| %VXLAN_OVERLAY_ROUTING_PROFILE_APPLIED: VxLAN Overlay Routing:   | Informational | Hardware overlay-routing-profile mode configuration is getting applied in the HW during system booting.   | No action required.   |
| <164>1<br>2021-09-09T06:07:07.470096+00:00<br>OS10 dn_alm 801 - - Node.1-<br>Unit.1:PRI [event], Dell EMC (OS10)<br>%POLICY_VXLAN_EGRESS_ACL_WARN-<br>ARNING: NVE configuration is<br>present on the switch. Do not apply<br>Egress ACL if this is a network<br>facing port on this VTEP ::access-<br>group name: ipv6Test | Warning       | A System log message is displayed on the console when an access-group is attached on the egress side of an interface when NVE is configured. This system log message appears only in the S5448F-ON and Z9432F-ON platforms. | Do not configure egress ACL on network facing ports in VTEP.        |

## IFM system log message reference

This section lists the system log messages that are generated by the IFM process.

**Table 61. IFM system log messages**

| System log message   | Severity      | Description   | Recommended action   |
|--|---------------|---|--|
| %IFM_OSTATE_UP: Interface operational state is up                              | Informational | Interface operational status is up.   | No action required.  |
| %IFM_OSTATE_DN: Interface operational state is down                            | Informational | Interface operational status is down.   | No action required.  |
| %IFM_ASTATE_DN: Interface admin state down                                     | Informational | Interface admin state down.   | No action required.  |
| %IFM_ASTATE_UP: Interface admin state up                                       | Informational | Interface admin state up.   | No action required.  |
| %IFM_PMBR_SPEED_MISMATCH: Port-channel member speed mismatch, disabled         | Informational | Port-channel member speed mismatch, disabled.                                     | Document the message exactly as it appears and contact technical support for assistance.   |
| %IFM_PMBR_SPEED_MATCHED: Port-channel member speed reset, admin state restored | Informational | Port-channel member speed reset, admin state restored.                            | No action required.  |
| %IFM_VINTERFACE_MAP_CREATED: Virtual interface map created                     | Informational | Virtual interface map created.  | No action required.  |
| %IFM_VINTERFACE_MAP_REMOVED: Virtual interface map removed                     | Informational | Virtual interface map removed.  | No action required.  |
| %IFM_PVLAN_SEC_VLAN_MAP : PVLAN  | Informational | Secondary VLANs does not exist or PVLAN mode not set, Mapping is inactive :vlan4. | Create the secondary VLAN using the <code>interface vlan &lt;vlan-id&gt;</code> command and configure PVLAN mode for the created VLAN using the <code>private-vlan mode community</code> or <code>private-vlan mode isolated</code> command. |
| %IFM_PVLAN_SEC_VLAN_DELETE PVLAN   | Informational | VLAN mode is not isolated community, primary VLAN mapping inactive.               | Configure PVLAN mode using the <code>private-vlan mode community</code> or <code>private-vlan mode isolated</code> command.  |
| %IFM_PVLAN_SEC_VLAN_MAP_DEFAULT_VLAN: PVLAN                                    | Informational | PVLAN configuration inactive on default VLAN.                                     | Change the default VLAN ID to some other VLAN ID, so that the applied PVLAN configurations on the older default VLAN remain effective.   |



**Table 61. IFM system log messages (continued)**

| <b>System log message</b>                                     | <b>Severity</b> | <b>Description</b>  | <b>Recommended action</b> |
|---|-----------------|---|---------------------------|
| % Error: Operation or its parameters exceeded IFM limitation. | Informational   | This System log message is displayed when the number of portchannels in the system exceeds 128. | No action required.       |

# Index

R

revision history [6](#)